CrossTalk

July 2006 The Journal of Defense Software Engineering Vol. 19 No. 7

net-centricity

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
CrossTalk: The Journal of Defense Software Engineering. Volume 19, Number 7, July 2006	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **OO-ALC/MASE,6022 Fir Ave,Hill AFB,UT,84056-5820**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

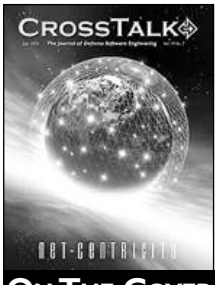
13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**32**	

Net-Centricity



On The Cover

Cover Design by Kent Bingham

Additional art services provided by Janna Jensen jensendesigns@aol.com

Departments

CrossTalk

76 SMXG Co-Sponsor	*Kevin Stamey*
309 SMXG Co-Sponsor	*Randy Hill*
402 SMXG Co-Sponsor	*Diane Suchan*
DHS Co-Sponsor	*Joe Jarzombek*
NAVAIR Co-Sponsor	*Jeff Schwalb*
Publisher	*Brent Baxter*
Associate Publisher	*Elizabeth Starrett*
Managing Editor	*Kase Johnstun*
Associate Editor	*Chelene Fortier-Lozancich*
Article Coordinator	*Nicole Kentta*
Phone	(801) 775-5555
E-mail	crosstalk.staff@hill.af.mil
CrossTalk Online	www.stsc.hill.af.mil/crosstalk

CrossTalk, The Journal of Defense Software Engineering is co-sponsored by the U.S. Air Force (USAF), the U.S. Department of Homeland Security (DHS), and the U.S. Navy (USN). USAF co-sponsors: Oklahoma City-Air Logistics Center (ALC) 76 Software Maintenance Group (SMXG), Ogden-ALC 309 SMXG, and Warner Robins-ALC 402 SMXG. DHS co-sponsor: National Cyber Security Division of the Office of Infrastructure Protection. USN co-sponsor: Naval Air Systems Command.

The USAF Software Technology Support Center (STSC) is the publisher of CrossTalk, providing both editorial oversight and technical review of the journal. CrossTalk's mission is to encourage the engineering development of software to improve the reliability, sustainability, and responsiveness of our warfighting capability.

S T S C

Subscriptions: Send correspondence concerning subscriptions and changes of address to the following address. You may e-mail us or use the form on p. 15.

517 SMXS/MDEA
6022 Fir AVE
BLDG 1238
Hill AFB, UT 84056-5820

Article Submissions: We welcome articles of interest to the defense software community. Articles must be approved by the CrossTalk editorial board prior to publication. Please follow the Author Guidelines, available at <www.stsc.hill.af.mil/crosstalk/xtlkguid.pdf>. CrossTalk does not pay for submissions. Articles published in CrossTalk remain the property of the authors and may be submitted to other publications.

Reprints: Permission to reprint or post articles must be requested from the author or the copyright holder and coordinated with CrossTalk.

Trademarks and Endorsements: This Department of Defense (DoD) journal is an authorized publication for members of the DoD. Contents of CrossTalk are not necessarily the official views of, or endorsed by, the U.S. government, the DoD, or the STSC. All product names referenced in this issue are trademarks of their companies.

Coming Events: Please submit conferences, seminars, symposiums, etc. that are of interest to our readers at least 90 days before registration. Mail or e-mail announcements to us.

CrossTalk Online Services: See <www.stsc.hill.af.mil/crosstalk>, call (801) 777-0857 or e-mail <stsc.webmaster@hill.af.mil>.

Back Issues Available: Please phone or e-mail us to see if back issues are available free of charge.

The Future Battlespace and the Power of Immediate Decision Making

Networks that are interoperable with Joint Forces will be fundamental to battlespace dominance in the future. FORCEnet, the Navy's architectural framework for that Joint interoperability, is geared towards providing naval aviation and surface platforms immediate access to images, signals, and data. The goal is to speed the flow of information, shorten the kill chain, and deliver a more effective use of weapons and firepower, allowing forces to conduct operations at a much faster pace, increasing effects-based warfare.

Adm. Michael G. Mullen stated in his 2006 Naval Sea Systems Command keynote address: We must design the fleet to support the network, and we must design the network to empower the fleet, and, to empower the fleet, the network must empower the sailor. The new littoral combat ship is a good example of how the Navy can design ships from the keel up around networks and sensors.

Adm. Mullen wants the same approach taken for all current and future ships, aircraft and submarines.

Whether developing an intranet infrastructure in Iraq or transforming communication systems in the Department of Defense (articles featured in this issue), key issues remain as how to provide a secure network with easy and immediate access to information that is accurate, valid, reliable, and relevant for the future battlespace decision maker.

FORCEnet enables the operational battlespace. In it, the enabling capability for a fully networked naval force is connecting to the similarly networked joint force that will be linked together by the Internet Protocol (IP)-enabled Global Information Grid. Our systems will be conceived, developed, and implemented as truly joint integrated capabilities capable of generating improved coalition effectiveness that will link warfighters ashore and at sea into a series of highly integrated distributed services networks capable of providing critical operational and tactical information to specified users. This will enhance naval capabilities to quickly make and execute decisions in the battlespace, synchronize the activities of widely distributed forces to mass effects on the enemy, and reduce threats to sailors and marines by providing broader situational awareness and operational flexibility. In this issue of CROSSTALK, there is a wide range of articles authored by those at the forefront of delivering the *Net-Centricity* of the future. From ground vehicles to data architecture, from the global grid to a focus on the strategic aspect of providing information access, the authors bring to life a forward-looking capability that is essential, fascinating, and complex.

Net-centric operations will distribute data and information to the warfighter across fault tolerant, adaptable, self-organizing, self-monitoring and self-healing, continuously available networks. A wide range of transmission paths, interoperable with those used by joint, coalition, civil, and law enforcement agencies, will be utilized. Warfighters embarking in net-ready aircraft, tanks, and ships will be able to communicate freely and autonomously down to the data-level while the underlying communications and network infrastructure will be invisible to the users. The infrastructure will also be readily deployable to any operating environment.

We cannot predict with certainty what specific threats we will face, but we do know we have to be flexible and globally intelligent, we have to operate jointly and at the same time seamlessly, and we must put the necessary information into the hands of those who need it precisely when it is needed. Entire systems at all levels of our government are being redesigned to meet this unpredictable future.

I imagine that as you read this issue of CROSSTALK you will look into our future with a new appreciation of net-centric efforts in place, that you will understand that our future threats go beyond the terrorist, and you may see your work in a new light.

Terrence Clark
Director, Software Engineering
Naval Air Systems Command

From the DoD CIO: The Net-Centric Information Enterprise

John G. Grimes
Networks and Information Integration
Department of Defense Chief Information Officer

Defense transformation hinges on the recognition that information is one of our greatest sources of power. Information can be leveraged to allow decision makers at all levels to make better decisions faster and act sooner. Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it most is the heart of the capability needed to conduct Net-Centric Operations.

Returning to the Pentagon after more than a decade, one immediately senses being in the midst of the most significant military transformation in over 50 years. The Department of Defense (DoD) is at the pioneering edge of the ever-expanding information frontier. Today's effort will lead to a capability that empowers every user and every decision maker to access timely, accurate, and trusted data. It will allow sharing of information and collaboration throughout the DoD's Net-Centric Information Enterprise and around the globe. The policies, systems, procedures, talent, and culture being developed will ultimately result in timely decisions and decisive actions across the defense team. As both a force enabler and a force multiplier, it will result in greater operational effectiveness based on enhanced awareness and deeper knowledge. Most importantly, today's work is critical to ensuring the nation's security, both now and in the future. Being on the team is exciting and a source of great pride.

As the DoD Chief Information Officer (CIO), my first and foremost commitment is to lead the effort that will deliver the critical enabling capability required by the National Defense Strategy to conduct Net-Centric Operations (NCO): We will conduct NCO with compatible information and communications systems, usable data, and flexible operational constructs [1].

Our objective is simple: connect people with information. The required enabling capabilities will allow users to select applications, data sources, and services to create a customized capability to perform a desired task.

The ability to reach all the way to the tactical edge of our operations is essential – regardless of time or location. Daily activities, mid-term planning, and long-term objectives must directly support the realization of this essential capability. By operating as a team, NCO will become a reality.

The Context for NCO

Less than two years into the new century the nation became painfully aware that early 21st century security challenges would be characterized by a single word: uncertainty. Uncertainty is the defining characteristic of today's strategic environment [1].

Our national security community must address unknown and asymmetric threats, a wide array of missions, unpredictable situations, and fast-paced operations. At the same time, the nation will face these challenges with partnerships and teams that cannot be anticipated and which will include other governments, business and industry, as well as additional non-governmental organizations. It will be impossible to predict what information will be needed, where it will be needed, who will need it, or when it must be accessed. More importantly, critical decisions will be made on ever-shorter time lines. And, the actions of a young soldier in the field can have strategic consequences felt around the world.

> *"Instead of pushing information out based on individually engineered and predetermined interfaces, net-centricity ensures a user at any level can both take what he needs and contribute what he knows."*

Prevailing, much less thriving, under these conditions will require unprecedented levels of flexibility, adaptability, creativity, and resiliency. We must *confront uncertainty with agility*. Creating a Net-Centric Information Enterprise is the path to agility. Users at all levels and in all situations can access the best information available, pool their knowledge, and make better decisions, faster. *I can get the information I need.*

Simply put, net-centric means people, processes, and technology working together to enable timely and trusted *access to* information, *sharing of* information, and *collaboration among* those who need it most.

Establishing *trust* is essential to creating the information environment of the future. Ensuring trust in the system (availability), trust in the information (assurability), and trust in the participants (identity) will be critical to success.

A Net-Centric Information Environment

Instead of *pushing information* out based on individually engineered and predetermined interfaces, net-centricity ensures that a user at any level can both *take what he needs* and *contribute what he knows*. Reaching that objective requires new methods of dealing with data – an information age approach.

The net-centric data strategy meets this challenge by focusing on *data* rather than on the proprietary applications and programs that manipulate it (the current focus). Users and applications post all data assets to *shared* space for use by others in the Net-Centric Information Enterprise, possessing an authenticated identity and an authorized access (role-based). Those at the source of the data will be required to make it easy to find and use. It must be *visible*, *accessible*, and *understandable*.

Key to the data strategy are the users who need information. Communities of interest (COI) are collaborative groups of users who must have a shared vocabulary

to exchange information. Data characteristics and content will be *tagged* in an agreed-to manner. The communities will range from pre-established groups with ongoing arrangements to unanticipated users and non-traditional partnerships that develop on an ad-hoc basis. Individual users will determine and display content based on their specific needs, user-defined operating pictures (UDOP) rather than in rigid or pre-determined formats.

Information assurance, the greatest Enterprise challenge, is the basis for *trust* – trust in the system's availability, the participants' identities, and the data's dependability and integrity. Today, firewalls and software patches attempt to keep intruders out and data safe. Tomorrow's assured information will require that the individual data be secured throughout its entire useful life span.

The Global Information Grid (GIG) exists to connect people with information. The GIG is the fundamental enabler for NCO. It collects, processes, stores, and manages the Enterprise data. The GIG is not just a technological backbone. It includes people, process, and technology.

The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, and managing information on demand to warfighters, defense policy makers, and support personnel. The information capabilities that comprise the GIG include transport, Web-based services, information assurance technologies, applications, data, and architectures and standards. It also includes the tools, techniques, and strategies for managing and operating the GIG (e.g., Network Operations). Operating the GIG enables *information on demand*.

Enterprise-wide system engineering (EWSE) function will provide the necessary guidance to ensure the successful introduction and continuing evolution of the GIG. Providing end-to-end interoperability and consistent performance is essential across the range of business, intelligence, and warfighting functions. The EWSE responsibilities include continuous oversight of the GIG's evolution, developing and maintaining the GIG technical baseline, establishing Enterprise-wide capabilities to support decision makers, implementing a program compliance management construct, and overseeing Enterprise-wide experiments. Creating a defense information Enterprise bears little resemblance to the platform-oriented programs of the past. Given the range of development responsibilities, diverse sets of potential users, and wide variety of needs, the path to success depends upon a holistic approach and an Enterprise-wide system engineering effort.

The DoD CIO

The DoD CIO provides the leadership to meet the net-centric vision and ultimately deliver the critical enabling capabilities required by the National Defense Strategy. *Delivering the power of information*, the DoD CIO vision will ultimately lead to an agile defense Enterprise empowered by access to, and sharing of, timely and trusted information. It is our mission to lead the information age transformation that will enhance the DoD's efficiency and effectiveness.

Transforming to a net-centric force requires fundamental changes in process, policy, and culture across the DoD (defense operations, intelligence functions, and business processes). As the CIO, three key objectives are essential to successfully enabling NCO.

> *"Developing the capabilities that will enhance today's operations and agility is crucial to those of tomorrow."*

First, *establish a true information age CIO*. Now is the time to establish a well-understood and institutionalized role for the DoD CIO. Specifically, the defense community must move out of the industrial age mentality that places computers, data, and their support in an administrative role. Instead, the institution must view information as a strategic asset. Information is the basis of knowledge and action. Timely, accurate, and trusted information lies at the heart of the capability to NCO. Developing the capabilities that will enhance today's operations and agility is critical to those of tomorrow.

Therefore, the CIO must be an inherent part of Enterprise-level policy and planning. It is the CIO's responsibility to ensure that the information necessary to operate the largest business in the world is always available when and where it is needed. The DoD CIO has the statutory authority to carry out his responsibilities. The current challenge is to translate those responsibilities into leadership across the Enterprise and transform to an information-centered environment.

Second, *tell a clear and compelling story of where the Enterprise is headed and why*. Unlike designing a tank or launching a satellite, transformation to NCO is traversing new ground. Today, the community stands at the brink of an era where networked capabilities will increase efficiency, enhance mission success, save lives, and potentially reduce force structure both at home and in theaters of operation. Information is a *force multiplier*. The implications are being felt today and even greater effects in the future can be anticipated.

The fundamental concept of net-centric warfare is very different from Cold War norms. Information can no longer be treated as a possession that is controlled by an owner. Stovepipe systems will not lead to agile information sharing. Information needs cannot be predetermined and they must support participation by unanticipated users. Today, the underlying approach and initiatives associated with net-centricity are both hard to explain and hard to understand. The entire community must do a better job of making sure that there is a common, clear, and consistent message. The message must establish both understanding of, and support for, the information environment that will enable successful operations in the future.

Third, *create a 21st century work force of information pioneers*. The DoD has embarked on the most significant change since the 1947 Key West Agreement restructured the Services. Transformation is not new. History reflects many examples of how new capabilities *enabled* operations previously impossible to imagine, much less conduct. The advent of the telegraph changed Civil War operations as did the radio 50 years later. Today, information networks are essential to enabling the agility needed to face uncertain and ever-changing challenges to our security.

However, this transformation will not occur if the *business as usual* mindset prevails. The DoD must have the requisite understanding and skills of an information age work force. More importantly, the entire Enterprise must excite, attract, and leverage the cutting-edge talent that it will take to reach the vision of NCO. This effort should be viewed as *the* most exciting and challenging work being done across both the public and private sectors. The excitement surrounding this transformation must draw in the very best and the very brightest and then keep them so engaged that they will not want to leave.

Coming Events

August 13-17
2006 AFITC Air Force Information Technology Conference
Montgomery, AL
https://ossg.gunter.af.mil/aq/AFITC/Default.aspx

August 14-17
ISHM 2006
2006 Integrated Systems Health Management Conference
Cincinnati, OH
www.usasymposium.com/ishm/default.htm

August 14-17
2006 Space and Missile Defense Conference and Exhibition
Huntsville, AL
www.smdconf.org

August 14-18
11th IEEE International Conference on Engineering of Complex Computer Systems ICECCS 2006
Stanford University, CA
www.iceccs.org

August 14-18
SICPP 2006
The 2006 International Conference on Parallel Processing
Columbus, OH
www.cse.ohio-state.edu/~icpp06

August 28-September 1
SecureComm 2006
Baltimore, MD
www.securecomm.org

April 16-19, 2007
2007 Systems and Software Technology Conference

www.sstc-online.org

Conclusion

Clearly, exciting challenges lie ahead. Success will rely on the ability to address Enterprise challenges as an integrated team. Ideas and capabilities from the private sector and academia are critical complements to efforts in the public sector. Collaboration, as in any undertaking, is key to success. Inspiring creative minds and innovative thinking must be Enterprise-wide. Therefore, the public-private partnership must continue to develop, evolve, and strengthen.

The technological change we have embarked upon will be significant, but the cultural shift may be even more challenging. The hallmark of the 21st century is uncertainty. Net-centricity is rooted in a simple principle: *confront uncertainty with agility*. To be agile, data can no longer be *owned*, it must be shared.

Timely and dependable information will be available across the Enterprise from higher level headquarters and command centers to a soldier tracking insurgents or a civilian in need of a new supplier. Ultimately, net-centricity means *power to the edge* – the ability to deliver the power of information across the entire Enterprise.◆

Reference

1. Department of Defense. The National Defense Strategy of the United States of America. Washington, D.C.: Mar. 2005 <www.globalsecurity.org/military/library/policy/dod/nds-usa_mar2005.htm>.

About the Author

John G. Grimes is the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. Previously, he served as Deputy Assistant Secretary of Defense for Defense-wide Command, Control, and Communications and was the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures. Grimes has held senior technical and staff positions with the National Communications System, Defense Communications Agency and the U.S. Army Communication's Command following his military service in the U.S. Air Force, and is the former Vice President of Intelligence and Information Systems of Raytheon Company. Grimes is a graduate of the U.S. Army War College, the Federal Executive Institute, and Harvard University's National and International Security Policy program, and is the recipient of two Presidential Rank awards.

6000 Defense Pentagon
Washington D.C. 20301-6000
Phone: (703) 695-0349
E-mail: john.grimes@osd.mil

Web Sites

Network Centric Warfare Department of Defense Report to Congress

www.dod.mil/nii/NCW

From the Department of Defense's (DoD's) Web site, the DoD's report to congress on the future of Network-Centric Warfare (NCW) is easily accessible. On this page, you can view a PDF or Word document of the report.

The Seven Deadly Sins of Network-Centric Warfare

www.nwc.navy.mil/WARDEPT/7deadl~1.htm

The Seven Deadly Sins of Network-Centric Warfare (NCW) can be found on the Naval War Colleges web site. This witty look at the potential problems and misconceptions of NCW offers great insight into the potential of creating NCW within naval forces and also points out looming mishaps. The following are the seven deadly sins of NCW: lust, sloth, avarice, pride, anger, envy, and gluttony.

Defense Information Systems Agency (DISA)

www.disa.mil/main/about/missman.html

DISA is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other Department of Defense components, under all conditions of peace and war. DISA is the provider of global net-centric solutions for the nation's warfighters and all those who support them.

Information Sharing Is a Strategic Imperative

General James E. Cartwright, USMC
United States Strategic Command

Americans are familiar with the host of new challenges posed by the forces of international terrorism, but one of the greatest threats we face may not be human at all, it may be a virus. John Barry's book "The Great Influenza" *details the flu pandemic of 1918 that killed more than 50 million people around the world. At one point, the flu spread so quickly that some government leaders feared a complete breakdown of civilization was only weeks away* [1]. *The Avian Flu might or might not turn into the next big threat, not only to the United States, but to its adversaries as well. The next big threat could be a natural disaster or something unanticipated.*

As the nation checks its horizon for the unexpected, it must not take its eyes off known threats and continue preparation for them. Both expected and unexpected cases require building a collaborative approach to face any threat America may face. As the realities of warfare and international security constantly evolve, the nation's strategy and willingness to work cooperatively must also evolve. There is a need for a collaborative approach among like-minded individuals and agencies to meet the challenges we face by merging our capabilities. A cultural change needs to take place across all the elements of international security to counter the threats faced today as well as tomorrow.

Successfully combating weapons of mass destruction (WMDs), for example, requires both military and civilian support to share technology and protect infrastructure. Failure to move beyond traditional boundaries risks sub-optimizing the potential for success. There is no alternative to establishing robust, collaborative relationships. The military, civil, and commercial interests of our nation all depend on the willingness to involve one another and fully enhance a shared worldview.

Facing Today's Adversaries

Among the challenges faced today are the unexpected, asymmetric methods that may be used by terrorists or other adversaries. These adversaries will not be reluctant to use WMDs: biological, chemical, or nuclear. Meeting the threat requires the ability to reach across all of the nation's security and defense elements to leverage the potential of America's economic and military infrastructure. This coordinated network must be able to effectively employ capabilities against any adversary.

The nation's economy, quality of life, and defense structures are all linked together in a global tapestry. The price of coffee and oil, a story on Al Jazeera, or a tsunami on the other side of the planet all have direct impact on daily life in this global environment.

Net-Centric Integration

Because America's vital military and economic interests are at stake, net-centric integration of our defense and security options provides a strategic advantage to face asymmetric threats. For its part in developing new approaches to integrate and synchronize actions, empower subordinates, and increase operational speed, U.S. Strategic Command (USSTRATCOM) is moving forward on two fronts. The first is re-tooling organizational and informational structures to make better use of all resources. The second front is actually more difficult. It involves changing the way human beings think about things and the military's basic cultural approaches to problems.

> *"The nation's economy, quality of life, and defense structures are all linked together in a global tapestry. The price of coffee and oil, a story on Al Jazeera, or a tsunami on the other side of the planet all have direct impact on daily life in this global environment."*

USSTRATCOM is transforming both old culture and old structure. One of the command's contributions in the world of information assurance (IA) and net-centric operations involves blogging on the newly installed Strategic Knowledge Integration-Web (SKI-Web) network. On my orders, any airman, seaman, or private first class can blog information on SKI-Web. Contributors buy their way into the blog with the value added – not the rank held. *Stars* and *stripes* are both welcome. Waiting for perfect information that plods through the same old napoleonic structure can make decisions irrelevant in today's world. To be effective, however, culture change also requires altering organizational constructs.

USSTRATCOM is also rebuilding its structure by establishing Joint Functional Component Commands (JFCC) that align responsibilities and authorities, decentralize operational execution, and increase operational speed. JFCCs are manned by STRATCOM planners and operators taken from our headquarters staff. Rather than build new organizations, JFCCs work side-by-side with and take full advantage of already existing centers of excellence that have complementary expertise and authorities.

JFCC Network Warfare (JFCC-NW)

JFCC-NW is collocated with the National Security Agency (NSA), and the commander of JFCC-NW is dual-hatted as the director of the NSA. While the structure has changed, real success requires alterations in culture. Military and government civilian teams must get used to doing business together rather than remaining in their old, comfortable lanes. They must establish

new lines of communication and new lines of authority. Both sides must be onboard to determine what procedures are required for mission execution and their joint role in IA. This effort is critical to supporting efforts to integrate and distribute the data that drives knowledge and ultimately action.

For information capabilities to be of real value today, warfighters must be able to *plug and play* in a joint global environment. Acquiring the ability to plug and play requires revolutionizing the mechanism for consistently incorporating information technology, controlling the configuration of technical components, and ensuring compliance with technical *building codes*. Professionals must constantly review the architectures necessary to provide this vital mechanism as it serves warfighters.

In this endeavor, JFCC-NW has a full partner in Joint Task Force Global Network Operations (JTF-GNO), now collocated with the Defense Information Systems Agency (DISA). The JTF-GNO commander also serves as the Director of DISA. Together they are treating networks as if they were a weapons system because they are certainly an extension of warfighting efforts. That fact is reflected in the training designed today as well as in the standardization of processes. In its current incarnation, JTF-GNO has been around for less than two years. It reflects a belief that the people operating networks should be the same people who defend those networks.

JFCC-Space and Global Strike (SGS)

As for USSTRATCOM's other mission areas, JFCC-SGS is responsible for integrating planning and command and control (C-2) support for the rapid delivery of extended range, precision effects in support of theater or national objectives. SGS mission responsibilities now require the capacity to rapidly and accurately reach any adversary on the planet with kinetic or nonkinetic effects. JFCC-SGS is led by the same three-star general who commands the 8th Air Force – a large part of USSTRATCOM's *global strike* arm. SGS plans global strike activities and serves as lead integrator of joint effects across the range of USSTRATCOM's capabilities. SGS also runs STRATCOM's Global Operations Center and serves as the commander's eyes and ears for situational awareness.

With the merger of the former with Space Command in 2002, the new STRATCOM also directs the deliberate planning and execution of assigned space operation missions. A new Joint Space Operations Center (JSpOC) has stood up, led by the same two-star general who commands the 14th Air Force – the largest part of STRATCOM's space arm. Establishment of the JSpOC and designation of a Commander, Joint Space Operations (JSO), brings true joint perspective and capability to the space operations world. The JSpOC cuts across boundaries to direct all elements of DoD space capabilities from daily space operations through space support to the regional combatant commands.

> *"It will take a team effort to meet challenges on issues as complicated as international treaty interpretation and as basic as the safety of our nation's food supply."*

JFCC-Integrated Missile Defense (IMD)

JFCC-IMD is headquartered in Colorado Springs, Co., to take advantage of missile defense activities located there. The commander of JFCC-IMD is dual-hatted as the commander of Army Space and Missile Defense Command. While the Missile Defense Agency has the specific assignment to develop missile defense systems, it continues to be the job of JFCC-IMD to offer a warfighter's focus and make the system operational by planning, integrating, and coordinating global missile defense operations and support (sea, land, air, and space-based).

JFCC-Intelligence, Surveillance, and Reconnaissance (ISR)

JFCC-ISR plans, integrates, and coordinates intelligence, surveillance, and reconnaissance in support of strategic and global operations and strategic deterrence. This includes coordinating ISR capabilities in support of global strike, missile defense, and associated planning. JFCC-ISR is collocated with the Defense Intelligence Agency (DIA) and the commander of JFCC-ISR is dual-hatted as the director of DIA.

Success in today's environment requires effectively coordinating all intelligence collection capabilities. The information collected must then be made available to a wide range of customers based on a secured *need-to-share* basis rather than the old *need-to-know* threshold.

Combating WMDs

In January 2005, USSTRATCOM was assigned the mission of integrating and synchronizing DoD efforts to combat WMDs and has looked to the Defense Threat Reduction Agency (DTRA) as a partner. The new WMD center is modeled on the other JFCCs, but is headed by a civilian director – in this case, dual-hatted as the director of DTRA. The first priority is rapidly advocating development and implementation of capabilities to support interdicting and eliminating WMD and its related materials. Since terrorists do not distinguish between America's civilian and military establishments, the nation must look at potential military and civilian targets and vulnerabilities alike. The WMD center links military interests with private industry leaders to share information, assess vulnerabilities, and develop deterrent, detection, and response capabilities. It will take a team effort to meet challenges on issues as complicated as international treaty interpretation and as basic as the safety of our nation's food supply. America is truly a nation at war, and private industry is certainly doing its part in supporting USSTRATCOM's newest mission area.

The Challenge of Change

As USSTRATCOM integrates joint, geographically separated, interdependent operations, technical issues must be worked out. However, the greatest challenge to building global integration will be achieving the cultural change referred to earlier in this article. This cultural change is not optional. It must occur in order to build a responsive command that can truly reach across multiple organizations and missions to deliver integrated joint effects. Everyone understands the need for change until it affects him or her personally. But moving further into the 21st century requires replacing *need to know* with *need to share* to achieve the full

strategic potential of net-centric operations. That means partnerships must grow and mature as the military, government, civilian, and industrial communities build on a long history of cooperation to optimize both current and future issues of interoperability. These partnerships must include the nation's best minds and resources in academia and private industry, as well as coalition partners and both the civilian and military sides of government.

Success requires adopting data-tagging standards and IA policies to increase government-wide, trusted information sharing. It requires supporting dynamic, persistent, trustworthy, collaborative planning, with user-defined operating pictures, using distributed, globally available information. The command is not there yet. But thanks to professionals in the military, government service, and private industry, USSTRATCOM is improving its global capabilities. That, in turn, will allow America's defense and security structure to take full advantage of the culture change as it evolves. To deliver the capabilities needed to combat the threats of the 21st century, USSTRATCOM is rebuilding and restructuring America's national C2 apparatus through a growing system of operation centers. Building these joint, geographically separated, interdependent operations meets our imperative need to pursue high capacity, Internet-like capabilities. It creates an indestructible C2 network as it extends the Global Information Grid to deployed and mobile users worldwide. This is vital to maintaining our traditional global deterrence at the same time we move all mission operations at the speed of light through high-capacity, virtual collaborative networks. The men and women who serve this command are aggressively moving out on actions to ensure USSTRATCOM fulfills its full set of global responsibilities, supporting national security needs in peace and in war.◆

Reference

1. Barry, John M. "The Great Influenza: The Epic Story of the Deadliest Plague in History." Penguin Group: New York, NY: 2004.

About the Author

General James E. Cartwright has served as commander, U.S. Strategic Command, Offutt Air Force Base, Neb. since July 2004. He leads an organization involved in the global command and control of U.S. strategic forces to achieve critical national security objectives. During his 35-year Marine Corps career, Cartwright held several operational and staff posts including commanding general, First Marine Aircraft Wing, and director, Force Structure, Resources and Assessment, J-8 the Joint Staff. As a pilot, he has flown the F-4, OA-4, and F/A-18.

United States Strategic Command
Office of Public Affairs
901 Sac BLVD STE 1A1
Offut AFB, NE 68113
Phone: (402) 294-4130
E-mail: hollanju@stratcom.mil

More Online from CrossTalk

CrossTalk is pleased to bring you these additional articles with full text at <www.stsc.hill.af.mil/crosstalk/2006/07/index.html>.

The New Java Security Architecture

Idongesit Mkpong-Ruffin and Dr. John A. Hamilton, Jr.
Department of Computer Science and Software Engineering
Auburn University
Dr. Martin C. Carlisle
Department of Computer Science
United States Air Force Academy

Java's original security architecture was designed to facilitate executing software from remote systems while simultaneously preventing downloaded code from performing unauthorized operations on host machines. The sandbox model of the Java Development Kit 1.0's security architecture was found to be too restrictive; therefore, the model was modified so that remote code could be allowed as trusted code. In the Java 2 platform, the notion of trusted code was removed and security control mechanisms were implemented that could be applied to both application and applet code so the code could be run with configurable trust. Java developers need to understand and incorporate the new Java security architecture into their development process to make certain their applications are secure. This article looks at the implementation of the new architecture and the new mechanisms provided for ensuring security for Java code. It details the motivation for the security changes in a security architecture, gives a general overview of the architecture added, and looks at some of the details of the mechanisms either changed or provided by the new architecture.

Software Cost Estimating: A Cyclical Conundrum

Ellen Walker
Data and Analysis Center for Software

This article describes the dilemma of some organizations in establishing credible software estimates, proposes some guiding principles and practices for improving the process, and addresses how current software best practices may play a role in the journey to achieving accurate software estimations. It seems that in spite of acquisition reform, in spite of our decade-long focus on achieving software process maturity, in spite of our adoption of modern structured development approaches, we (the software acquisition/development community) still have problems achieving success (defined as delivering a quality product on time and within budget). Perhaps the incentives are not strong enough to compel us to deliver quality. Perhaps our focus is skewed in favor of cost or delivery time over quality. Perhaps our cost estimating practices (or lack thereof) are impacting our success with software development. The hundreds of articles on software estimation and software metrics, and hundreds of hours spent in research and development of estimation techniques have not focused on the people and cultural issues surrounding estimating and data collection. Consequently, the reality of cost estimating and perceptions of practioners toward it, are, for the most part, vastly different from what the literature describes.

Secure From the Start: Designing and Implementing an Assured National Security Enterprise

LTG Keith B. Alexander
National Security Agency/Central Security Service

The Global Information Grid (GIG) information assurance (IA) architecture is the embodiment of an Enterprise IA model and is being designed to support the entire National Security Enterprise with input from the Department of Defense, Department of Homeland Security, and intelligence community. It is an essential enabler of the GIG Net-Centric Warfare vision. National Security Agency (NSA) architects have identified innovative IA approaches to support dynamic, secure enterprise-wide information sharing. Portfolio management for the effort is being provided by the GIG IA Portfolio Management Office at NSA in partnership with Office of the Secretary of Defense, and the Military Services, commands and agencies.

The Global Information Grid (GIG) is a Department of Defense (DoD) initiative to develop an assured global information technology (IT) enterprise that will enable its strategic objectives of information superiority and net-centric warfare (NCW). NCW is a set of warfighting concepts and capabilities that provide for worldwide access to information and services – anytime, anyplace – allowing the warfighter to take full advantage of all available information and bring all available assets to bear on the mission in a rapid and flexible manner. To achieve this vision, the DoD is transforming the way it operates, communicates, and uses information to include expanding user access to a much richer set of information and collaboration capabilities. Information assurance (IA) is a critical enabler of the GIG and the DoD strategic objectives.

Roles and Responsibilities

The National Security Agency/Central Security Service (NSA/CSS) is an active participant, partner, and leader in making net-centricity a reality. Due to NSA/CSS's unique position of performing both offensive and defensive missions, the Assistant Secretary of Defense for National Information Infrastructure (ASD/NII) tasked NSA/CSS to provide the IA architectural guidance and IA portfolio management to deliver the DoD's GIG vision. We are partnering with U.S. Strategic Command (STRATCOM), the Joint Staff, the Defense Information Systems Agency (DISA), and the Military Services in defining and implementing a secure, net-centric operating environment. Additionally, we are working with the intelligence community (IC) to drive the increased sharing of critical data securely.

The NSA/CSS's Enterprise IA Architecture and Systems Engineering Office, in partnership with the GIG community, leads the effort to define a GIG IA architecture that includes enterprise-level IA strategies, guidance, standards, policies, systems requirements, and technologies necessary to realize DoD's net-centric GIG vision. While the office's principal focus is on supporting the GIG, its work is broadly applicable to net-centric enterprise efforts across the IC, Department of Homeland Security (DHS), Information Sharing Environment (ISE), and other federal information technology (IT) enterprises. These national security communities require the development of an assured global national security IT enterprise to transform the way they operate, communicate and use information to accomplish their missions. NSA/CSS's IA support will help ensure that communications, information sharing, and infrastructure availability are not barriers to the nation's security.

> *"Dynamic interactions in a net-centric collaboration and information-sharing environment require a greater level of interdependency between systems."*

IA Vision

The DoD net-centric IA vision is to enable a dynamic, information-sharing environment that delivers secure information at the right time, to the right recipient, and in the right format under every circumstance. This environment must be securely managed and protected enterprise-wide from threats posed by adversaries. Providing enterprise-wide protection of the dynamic information-sharing environment requires a cohesive, integrated approach to IA that enhances policies, procedures, technologies, and training.

Enterprise IA Model

In the past, a system-high security approach was taken to secure the system containing the information. The system-high security model requires the system to operate at the level of the highest information classification and the protection mechanisms be approved to protect the highest classification level of information contained within the system. Additionally, every user had to be cleared for that level of access (i.e., if the highest classification of information being processed in a system is SECRET, then all the systems and interconnections involved in sharing this information need to be protected and need to meet the security requirements for protecting SECRET information).

Dynamic interactions in a net-centric collaboration and information-sharing environment require a greater level of interdependency between systems. The traditional system-high security approach cannot be used to support dynamic interactions between systems in this variable environment. The dynamic interactions occur in an environment where trustworthiness

varies between the users participating in the collaboration and sharing, the systems supporting the collaboration and sharing, and the sensitivity levels of the information being shared. These collaborative users form groups commonly referred to as communities of interest (COI). A COI is any group of users that needs to exchange information to accomplish a given mission. COIs may be pre-established users with ongoing agreements, or may develop on an ad-hoc basis and may include both traditional (e.g., coalition forces for military engagements) or non-traditional partners (e.g., federal, state, or local government agencies in support of disaster relief missions). The dynamic interactions require that the protection approach for information sharing shift to a transaction-based *Enterprise IA model*.

Under this new model, information exchanged as part of a transaction is protected to a level appropriate for the information being exchanged. That is, dynamic mechanisms are used to determine whether or not information should be shared and under what conditions. The approach to realizing the assured GIG vision is shaped by the following set of guiding principles essential for the transformation of IA:

- **Separation of Information Protection from Infrastructure Protection** (i.e., protecting information wherever it resides). Past IA models focused predominantly on protecting the physical computing and data storage devices and their communications infrastructure (e.g. gates, guards, dogs, and link/network encryptors). Net-centric IA will augment and evolve current communication infrastructure protections to allow for a dynamic, distributed perimeter where end-to-end object-level information protection reduces (and perhaps eventually replaces) the physically separate networks used across the community today. This includes protecting data in storage, packets, messages, and sessions in transit in addition to the networks.
- **Policy-Driven Enterprise.** The impacts of system outages, degradations, and cyber attacks will significantly expand in the net-centric environment. Interdependence and interconnection of systems will affect our ability to contain these impacts. A digital policy driven enterprise that enables dynamic, highly automated and coordinated establishment and enforcement of information access, mission priority, resource allocation, and cyber attack response will counter this increased threat. It will also provide the ability to adjust resources to ensure that the highest priority missions receive the resources needed for their success.
- **Support for Varying Levels of Trust.** Today we define a single standard for protection of information that resides within a system-high environment. As we move forward into the highly interconnected net-centric environment, the enterprise will need to ensure information is sufficiently protected while supporting collaboration and information sharing across environments where the users and their systems have varying levels of trustworthiness.

"We must develop and apply robust tools, technology, and operational approaches to actively defend our networks."

- **Persistent Monitoring and Misuse Detection.** Counterbalancing the increased cyber and insider threats brought about by the broader sharing and greater interconnectivity of systems requires enhanced cybersituational awareness and network defense capabilities. We must develop and apply robust tools, technology, and operational approaches to actively defend our networks. A key part of this strategy is to shift to a distributed enterprise sensor grid, in which IT components throughout the enterprise provide sensor inputs. Persistent monitoring develops cybersituational awareness through analysis of the sensor grid inputs across classification levels, missions, and COIs. This capability is critical to improving the ability to detect misuse and insider threats.
- **Greater Use of IA-enabled IT Components.** Today's IA capabilities are implemented in a bolt-on approach (e.g. add-on security products) as specialized IA appliances primarily deployed at the enterprise perimeters. The Enterprise IA model requires IA functionality to be distributed across IT components as well as greater reliance on software-based IA functionality combined with greater assurance and trust in the host computing platforms. This new enterprise protection model *bakes in* IA functionality by requiring it to be designed and built into IT components from their inception, and requires increased trustworthiness in those components to correctly perform their IA functionality. The terms *bolt on* and *baked in* are diametrically opposed. Bolted-on security implies that it has been added after the fact. Baked-in security requires that the security features be designed and integrated throughout the system lifecycle, from concept. *Baked in* is inherently superior because it guarantees that complementary, mutually supportive approaches and technologies are employed.
- **Evolution to Dynamic Security Management.** Today, the management of security is primarily focused on the generation and distribution of public key certificates and cryptographic keys for cryptographic devices. In an environment where enterprise protection relies on an array of IA-enabled IT products, the concept of security management must expand to support not only a more automated, net-centric key management capability, but it must also evolve to support security services such as identity, privilege, audit, and IA configuration management. With the development of a more comprehensive toolkit of security management capabilities, they can be applied to support the active defense of our networks by dynamically reconfiguring access to network resources as directed by network security policy and informed by persistent monitoring and situational awareness.

GIG IA Architecture

The GIG IA architecture is the embodiment of the *Enterprise IA model* into a set of architectural products (e.g., operational, system, and technical views) that defines the IA strategies and capabilities to ensure protection

of the information, availability, and assured control of the GIG IT infrastructure. Assured operation in the high-risk, end-state environment of the GIG will require unprecedented changes to its information, services, and infrastructure. Full integration of IA solutions, with the appropriate IA functionality and robustness within nearly every IT component of the GIG enterprise, will be paced by resources and commitment. Thus, over the next decade, the GIG enterprise will undergo an incremental evolution toward the end-state vision with new IA capabilities phased in as operations, technologies, resources, and policy permits. The gap between the near-term capabilities and the end-state vision will be bridged through one or more incremental rollouts of interim IA capabilities. The GIG IA architecture strategy will serve as the foundation for delivering IA capabilities to the IC, DoD, NSA/CSS, DHS, ISE, and other federal agencies comprising the National Security Community.

GIG IA Portfolio Management: Implementing the GIG IA Architecture

On October 10, 2005, the Deputy Secretary of Defense approved the DoD IT Portfolio Management Directive, otherwise referred to as DoD Directive 8115.01. This directive dramatically changes the way that DoD manages major initiatives and the projects that comprise them. To comply with the guidance referenced in the introduction, the DoD Chief Information Officer (CIO), as the Enterprise Information Environment Mission Area (EIEMA) lead, established Enterprise Information Environment domains, and named domain owners, including the Office of the Assistant Secretary of Defense/Networks and Information Integration as the domain owner for IA. The latter, in turn, appointed the Director, National Security Agency (DIRNSA) as the IA domain agent to lead the DoD's portfolio management IA activities. In September 2005, DIRNSA created the GIG Information Assurance Portfolio (GIAP) management office to execute these duties on his behalf. Though located at NSA/CSS and initially staffed with NSA/CSS personnel, this is a community office and will eventually grow to include other community members from across the national security community.

Developing an assured GIAP will not be *managing* all of the service and agency IA programs. That will be left to the services and agencies themselves. The GIAP has established a community-wide portfolio management working group to work closely with ASD/NII and its defense-wide IA program office, and representatives from STRATCOM, Joint Staff, DISA, and the Services to examine the IA programs to determine the capabilities they deliver and the capabilities they are depending on to achieve success as well as at the timing of the programs to ensure they are aligned. This synchronization is important to ensure that DoD dollars are being invested optimally.

"The GIG is an exciting and challenging undertaking that will need participation and partnership by the DoD, IC, DHS, industry, and academic communities."

The GIG is an exciting and challenging undertaking that will need participation and partnership by the DoD, IC, DHS, industry, and academic communities. NSA/CSS has defined a *defense-in-depth* IA strategy that relies on intrinsic, baked-in security and dynamic management, which focuses on protecting information in addition to the communications networks. That, along with extrinsic testing and analysis of residual risks and implemented with sound network security design, provides effective 24/7 operations.

NSA/CSS continues to contribute to the information sharing needs of the men and women serving in harms way, actively fighting terrorism, and defending our country. NSA/CSS has committed senior-level managers, technical leaders, and a deep cadre of technical experts to make the GIG vision, through the GIG IA architecture and portfolio management, a success.◆

Information Sources

1. Department of Defense Directives: <www.dtic.mil/whs/directives>.
2. Department of Defense Global Information Grid: <www.defenselink.mil/nii/global_Info_grid.html>.
3. Department of Defense Global Information Grid Information Assurance: <https://gesportal.dod.mil/sites/gigia>.

About the Author

LTG Keith B. Alexander, USA, is the Director, National Security Agency/Chief, Central Security Service (NSA/CSS), Fort George G. Meade, Md. As the Director of NSA and Chief of CSS, Alexander is responsible for a combat support agency of the Department of Defense with military and civilian personnel stationed worldwide. He entered active duty at the U.S. Military Academy at West Point. Among previous assignments, Alexander has served as Deputy Chief of Staff (DCS, G-2), Headquarters, Department of the Army, Washington, D.C.; Commanding General of the U.S. Army Intelligence and Security Command at Fort Belvoir, Va; Director of Intelligence, U.S. Central Command, MacDill Air Force Base, Fl; and Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, for the Joint Chiefs of Staff. He holds a Bachelor degree from the U.S. Military Academy, a Master of Science degree in Business Administration from Boston University, a Master of Science degree in Systems Technology (Electronic Warfare) and a Master of Science degree in Physics from the Naval Postgraduate School, and a Master of Science degree in National Security Strategy from the National Defense University.

National Security Agency
9800 Savage RD
FT George G. Meade, MD 20755
Phone: (301) 688-6524
E-mail: nsapao@nsa.gov

Service-Oriented Architectures in Net-Centric Operations

Lt. Gen. Charles E. Croom, Jr.
U.S. Air Force

Rapidly changing technology and the nature of military operations today and in the future necessitate a change in the way information is delivered to warfighters. Using a service-oriented architecture and proven acquisition techniques, the Defense Information Systems Agency will make information available to people faster, at reduced cost, and to a greater number of users.

Technology advances such as Web services and policy like the Department of Defense (DoD) data strategy are removing many of the barriers that have traditionally prevented information systems from easily sharing information [1]. *Service-oriented architectures* (SOAs) are frameworks that allow us to better use information by enabling formal and self-organizing communities with common goals or interests to develop and share information. SOAs also provide the ability to update, add, remove, and share information delivering services without having to interrupt or redesign missions or user interfaces. An SOA creates a framework that allows services to be used beneficially in new and powerful ways that could not be envisioned by the service developer. Good business practices aided by a successful SOA helps make an organization agile and eliminates many of the barriers that prevent business processes or mission areas from sharing and reusing information and services.

In the global war on terror, the United States faces an information age adversary. The Internet, wireless technologies, and mass media combined with decentralized organization and off-the-shelf weaponry provide our adversary with unprecedented agility and reach. Response to this threat requires exchange of actionable, high quality, and trusted information on an unprecedented scale. Making this information available requires a strategy that first, makes data visible, accessible, understandable, and trusted, and second, provides services to discover and deliver data securely.

Successful Businesses Get It

By implementing an effective service-oriented strategy, we expect to realize improved information awareness, better and faster decision making, and the ability to rapidly introduce new capabilities. Examples demonstrating the benefits of a successful service-oriented strategy can be found in the commercial world. In his book, "The World Is Flat," Thomas J. Friedman illustrates how an automated process to share information with suppliers increases information awareness and allows retailers such as Wal-Mart to dramatically reduce its inventories and increase overall efficiency. By effectively sharing information among its business processes, UPS is able to make better and faster decisions, constantly matching the deployment of their shipping to the flow of packages [2]. Low transaction costs allow online retailers, including Amazon and Netflix, to reach broader markets by offering products that stores requiring shelf presence cannot risk holding in their inventories [3]. Both Amazon and Netflix have recommendation services that use customer preferences and shopping habits to help customers discover and purchase niche products that would have otherwise gone unnoticed.

"The broad use of information technologies in commercial applications creates an environment where many technologies that meet warfighter needs already exist."

The DoD is no longer the clear leader in the world of information technology [2]. Low entry costs, a commercial market, and the global and egalitarian nature of the Internet have enabled companies and even individuals to develop and use technology faster and more efficiently than the military can. Businesses and private citizens are not constrained by acquisition processes designed to field weapon systems on 10-to-15 year time lines. At times, the current acquisition processes create artificial barriers that slow the acquisition of critical information capabilities.

Our Strategy

We intend to use an acquisition philosophy that improves our speed to market: *adopt before buy*, *buy before create*. This philosophy will allow us to rapidly incorporate capabilities that already exist. If another agency or military service has a solution that either fits or is close to fitting a need, it will be adopted in some fashion or other. If a solution cannot be found within our government, it may be possible to find a commercially available managed service that either fits or is close to fitting the need. In both cases, a risk analysis will determine if a service or capability meets a significant portion of the need. The analysis will identify what elements will not be satisfied and whether or not they are so crucial as to preclude adopting a pre-existing government solution or commercially managed service. It may be cost effective to use a second or third source to satisfy any critical elements that remain. If we cannot adopt or acquire a commercially managed service, we will create or build a solution, but it is our intention to avoid development when possible and turn to others for solutions when we can.

Acquisition oversight, testing, certification, and accreditation functions are required to ensure systems do what they are intended to do and ensure that tax dollars are used effi-

ciently. By working within this process, we can tailor it to make sure it delivers oversight commensurate with risk. The broad use of information technologies in commercial applications creates an environment where many technologies that meet warfighter needs already exist. They offer capabilities that have been operationally tested through months of use in the business world. We need to examine these capabilities on a case-by-case basis. Well performing, widely adopted offerings do not pose the same risk as new development and do not require oversight that is as expensive or time-consuming. Carefully matching oversight to risk allows our highly trained acquisition experts to focus their effort on higher risk acquisitions and delivers capabilities much faster.

The Defense Acquisition Performance Assessment conducted at the request of the Deputy Secretary of Defense noted that the addition of an *operationally acceptable* test evaluation category has the potential to accelerate delivery of key capabilities. The assessment identified examples where programs formally declared *not operationally effective* by the director of operational test and evaluation proved to be operationally useful in combat situations. Holding capabilities in testing to meet requirements that are not critical to combatant commanders effectively ties the hands of warfighters. We can deliver capabilities incrementally and provide value as soon as it is practical by introducing *schedule* as a key performance parameter, mandating delivery at specified intervals and developing the acquisition processes required to support it.

Again, businesses and individual users have operationally developed and tested capabilities that are applicable to DoD needs. Allowing them to be tested and fielded *as is* leverages commercial technologies and avoids circumstances where less critical requirements prohibit deployment of critical capabilities given appropriate security considerations [4].

We need to develop capabilities and services based on user feedback. Google uses feedback so efficiently that often times users set direction and help establish standards. Google's press center provides the following philosophy for product description:

> …centered on rapid and continuous innovation, with frequent releases of new technologies that we seek to improve with every iteration. We often make products available early in their development stages by posting them on Google Labs, at test locations online or directly on Google.com. If our users find a product useful, we promote it to *beta* status for additional testing. Our beta testing periods often last a year or more. Once we are satisfied that a product is of high quality and utility, we remove the beta label and make it a core Google product. [5]

This model embodies the speed, agility, and user focus that we need in a net-centric environment. We can meet the rapidly emerging needs of warfighters by using similar models that are fast and user-driven.

"By exposing users to services early and incorporating user feedback in the development process, service offerings will either die quickly or be transformed into something useful. User-focused development ... is clearly the way ahead."

The Defense Information Services Agency's Net-Centric Enterprise Services program established an initiative in September 2005 that provides a pre-production environment where users, service providers, and consumers can begin to familiarize themselves with net-centric services. Experimenting with services and capabilities in this way allows technical questions for streamlining the emerging acquisition strategy to be answered without expending the cost, time, and overhead of a traditional DoD program. Services developed like this can be started quickly at much lower costs and can be ended quickly when expectations are not met. By exposing users to services early and incorporating user feedback in the development process, service offerings will either die quickly or be transformed into something useful. User-focused development like this is clearly the way ahead.

Advantages of a Service-Oriented Architecture

Acquiring capabilities quickly and efficiently is only part of realizing a net-centric operating environment. These capabilities need to be implemented effectively. In adopting the SOA framework, the department will be able to make a set of core services available to all DoD users and developers. Versatile and reusable services with standard interfaces deliver more value than application specific code that *reinvents the wheel* in costly and sometimes unpredictable ways. The services work behind the scenes and act like glue to link and bind business and mission processes. Savvy users and developers can take advantage of these services, reusing them in unique ways and constantly aligning and binding processes to the overall mission. The SOA concept is not about technology; it is about synchronizing our processes to the mission.

Douglas K. Barry presents an example of how information services can reach across devices, business processes, and organizations to improve mission areas. His fictional sales representative is guided through a trip fraught with cancelled appointments and changing circumstances by information services. Machine-to-machine interactions using information services aid in trip planning, send directions to a global positioning system driving assistant in his rental car, update calendars, provide real-time notification of customer-reported problems, book hotels, and schedule flights. Additional information is available to the sales representative through mobile text messaging, palmtop storage, and instant messaging. The character's organization uses an SOA to deliver information from multiple sources both inside and outside of the organization, automatically re-synchronize reservations and appointments in response to changes, and notify the character on a variety of devices [6].

Furthermore, an SOA is in keeping with the fair and open competition that is an important part of the government acquisition policies. Well-defined, government-owned services that govern interaction between services provided

by different vendors would reduce ambiguity, reduce advantages inherent in long-standing contracts, and promote competition. The services can work together, can be produced by different vendors, can be produced and tested independently, and can be replaced without having to replace the entire system. In effect, this reduces information services to commodities. Doing so lowers costs, speeds acquisition, and allows vendors to distinguish themselves by offering superior services instead of watching another vendor charge the government recurring patch and upgrade costs on proprietary code.

Conclusion

Rapid acquisition practices that provide oversight commensurate with risk are key to taking advantage of capabilities that, as a result of the Internet, are developed and adopted by businesses and individuals at an increasingly higher rate. SOAs provide a framework to apply new capabilities in ways that improve both individual processes and the way processes contribute to the overall mission. Businesses that *get it* have translated a strategy combining rapid acquisition and an SOA framework into industry leadership and greater success. The talent and creativity of the men and women in the department should be able to transfer these benefits to our military if we allow them.

The combined efforts of the Office of the Secretary of Defense, the Combatant Commands, the Joint Staff, military service chief information officers, and combat support agencies are required to match our acquisition processes to our environment, harness information with an SOA, and achieve net-centricity. We have and will continue to work together to change our processes to provide individuals who have chosen to defend their country every possible advantage.◆

References

1. Department of Defense Chief Information Officer. DoD Net-Centric Data Strategy. Washington, D.C.: Department of Defense, 2003 <www.afei.org/pdf/ncow/DoD_ data_strategy.pdf>.
2. Friedman, Thomas L. The World Is Flat. New York: Farrar, Straus, and Giroux, 2005.
3. Anderson, Chris. "The Long Tail." Wired, Oct. 2004.
4. Kadish, Ronald, et al. "Defense Acquisition Program Assessment." Defense Acquisition Performance Assessment Project. Washington, D.C.: Department of Defense, Jan. 2006. <www.acq.osd.mil/dapaproject/documents/DAPA-Report-web.pdf>.
5. Google Press Center. "Press Center." <www.google.com/intl/en/press/descriptions.html>.
6. Barry, Douglas K. Web Services and Service-Oriented Architectures. San Francisco: Morgan Kaufman Publishers, 2003.

About the Author

Lt. Gen. Charles E. "Charlie" Croom Jr. is Director, Defense Information Systems Agency (DISA), and Commander, Joint Task Force - Global Network Operations (JTF-GNO). DISA plans, develops and provides interoperable command, control, communications, computers and information systems to serve the needs of the Department of Defense (DoD) under all conditions during peace and war. As the JTF-GNO commander, Croom is responsible for directing the operation and defense of the Global Information Grid to assure timely and secure net-centric capabilities across strategic, operational and tactical boundaries in support of the DoD's full spectrum of warfighting, intelligence, and business missions. He has held four commands and has served at the major command, numbered air force, Air Staff, defense agency, Joint Staff, Office of the Secretary of Defense, and unified command levels. Croom has a Bachelor of Science degree in electrical engineering, a Bachelor of Arts in economics from Rutgers University, a Masters degree in management and business from Webster College, and completed the John F. Kennedy School of Government Executive Program at Harvard University.

Defense Information Systems Agency
P.O. Box 4502
Arlington, VA 22204-4502
Phone: (703) 607-6001
Fax: (703) 607-4078
E-mail: charles.croom@disa.mil

Tuesday's first-ever government and industry executive panel included (left to right) moderator Dr. Jim Kane, president and CEO of Systems and Software Consortium; Sean Bond, vice president and general manager of Aerospace Controls BAE SYSTEMS Electronics and Integrated Solutions; Terry Jaggers, Secretary of the Air Force/AQR; Hal Wilson, senior director and chief engineer, Northrup Grumman Mission Systems Defense Mission Systems Division; Carl R. Siel, Jr., Assistant Secretary of the Navy, Chief Engineer; Mark D. Schaeffer, acting director, defense systems director, systems engineering OUSD (AT&L); and Dr. Art Pyster, senior vice president and director of systems engineering and integration, SAIC.

Transforming: Business, Security, Warfighting Themed the 2006 Systems and Software Technology Conference

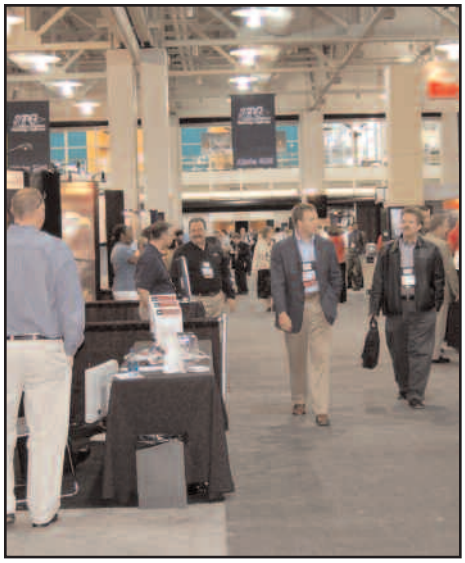
Defense leaders and industry professionals gathered in Salt Lake City from May 1-4 at the annual Systems and Software Technology Conference (SSTC) to share and improve methods of transformation throughout the U.S. military. From the floor of the diverse trade show to the podiums of the general sessions and expert presentations, the goal of the conference to contribute to the enhancement of the attendees' professional skills and knowledge of systems and software technologies delivered insights into the value of transformation in business, security, and warfighting.

The SSTC offered professionals and attendees the opportunity to engage in conversation with the aim to improve and implement the newest best practices in the areas of software technology and military advancement by creating an environment of open discussion at the speaker luncheons, plenary sessions, and exhibitor tracks.

Participants gleaned valuable information and lessons learned from more than 175 presentations and tutorials offered in seven concurrent tracks, including agile development, architecture, future technologies, information assurance, information technologies, project management, and net-centricity. SSTC attendee Paul E. McMahon found that the conference helped improve his productivity:

> Over the past few weeks, I have started a number of times to write a new CROSSTALK article, but got stuck because I wasn't sure what I was going to say. During SSTC, after I gave my presentation on Monday, a number of people stopped me and asked good questions about agile, which caused further thoughts and more notes in my pocket. On Wednesday, I listened to James Sutton speak and he made one particular point that caused the wheels to turn faster. At the CROSSTALK author luncheon, I had an interesting discussion with Doug Parsons, which continued the next morning at his presentation on combining traditional and agile development. And then, Judy Bamberger, in the second to last presentation of the conference, hit the final point I needed. I literally wrote a complete article flying home on Friday. My reason in relaying this story is the following: Sometimes we think we are too busy to go to a conference or write an article or review someone else's material. But the reason I keep coming to SSTC and the reason I keep writing articles for CROSSTALK is because it always ends up making my workload easier rather than harder. The information I acquire by listening to others, reading their work, and discussing real situations during the SSTC has helped me solve some dilemmas I have been facing with a current client. So, on top of everything else, I am actually ahead of schedule! I wish that more people understood that the secret to productivity is going to SSTC.

The SSTC, co-sponsored by United States Army, United States Marine Corps, United States Navy, Department of the Navy, United States Air Force, Defense Information Systems Agency, and Utah State University, brings together experts from academia, industry, and the Department of Defense. This coalition of knowledge opens doors to future software technology endeavors by providing productive networking opportunities from the opening to the closing session.



The trade show offered SSTC attendees a chance to see the latest systems-related technologies.

Grady Booch, a recipient of the Stevens Lifetime Achievement Award, addresses the conference opening general session.

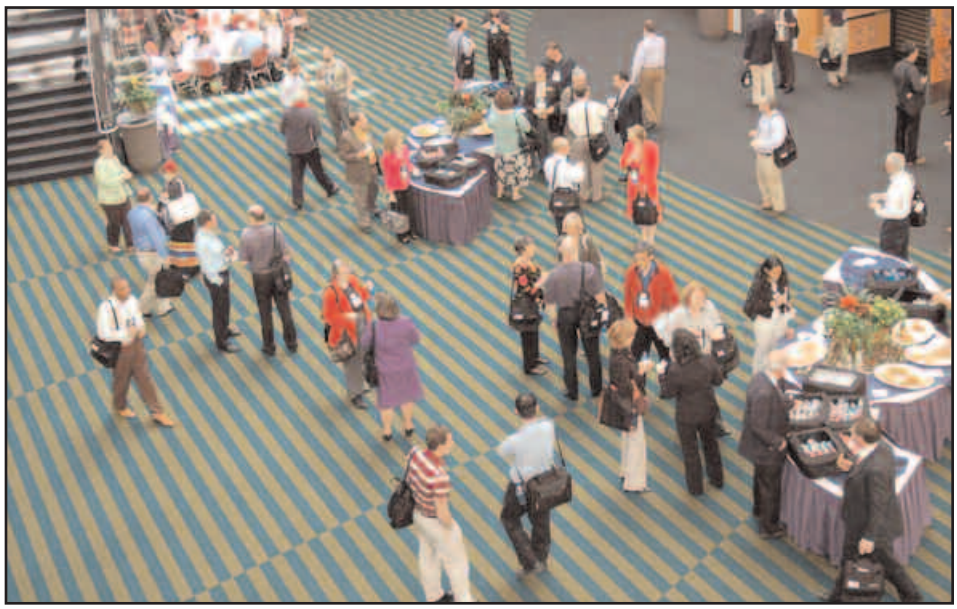
SSTC attendees enjoyed the lighthearted comedy of the Bar J Wranglers performance during Wednesday evening's entertainment, which also included a chuckwagon dinner.

> *"... the reason I keep coming back to SSTC ... is because it always ends up making my workload easier rather than harder. The information I acquired by listening to others, reading their good work, and discussing real situations ... has also helped me solve some dilemmas I have been facing with a current client."*
>
> — *Paul E. McMahon*
> *SSTC attendee*

Photography by Bill Orndorff

Gen. Bruce Carlson, U.S. Air Force Materiel Command, and Capt. Paula Ross greet Utah State University President Stan Albrecht.

Impromptu side meetings like this one were a common sight between sessions.



SSTC attendees take a break in between one of many tracks at the Salt Palace Convention Center.

The Team: Creating the Enabling Capability to Conduct Net-Centric Operations

Lt. Gen. Robert M. Shea
Command, Control, Communications, and Computer Systems

The ongoing transformation of the Department of Defense demands new capabilities that will enable Network-Centric Operations (NCO). While the Joint Command, Control, Communications and Computer (C4) systems community has been working toward this vision, emphasis has had to shift to a detailed plan to attain it. As a result, a critical task of the Director, C4 Systems Directorate, and the Joint Staff has been to provide the joint C4 community with a unifying strategy that would better integrate and synchronize our collective Joint C4 efforts and staff actions and deliver the C4 capabilities that will enable Joint NCO. After working with and receiving feedback from various Office of the Secretary, Combatant Command, Service (i.e., Army, Navy, Air Force and Marines) and Agency partners, the directorate delivered that strategy in 2004: the Joint C4 Campaign Plan.

2005 focused on the implementation of the Joint *Command, Control, Communications and Computer* (C4) campaign plan. As a result of these efforts, substantial progress has been made toward contributing to the delivery of critical, enabling C4 capabilities and preparing for future Network-Centric Operations (NCO). We are committed to ensuring that 2006 will be an equally productive year.

Accomplishments in 2005

Development of a contextual framework (concept documents) has been critical to supporting the review and approval of new capabilities as they moved through the Joint Capability Integration and Development System (JCIDS) process[1]. In support of this need, in 2005 the Joint Requirements Oversight Council (JROC) approved two critical C4 concept documents: the Net-Centric Environment Joint Functional Concept (NCE JFC), and the Net-Centric Operational Environment Joint Integrating Concept (NCOE JIC)[2]. The NCE JFC defines baseline functional capabilities and attributes required for NCO and will drive capabilities based assessments (CBAs) by identifying network-centric gaps and shortfalls. This analysis will ensure senior decision makers field future C4 capabilities that will *truly be born Joint*. The NCOE JIC will extend the NCE JFC's integrating framework, helping to establish the conditions, tasks, and standards needed to support CBAs that will define the specific net-centric needs of our future joint force. Together, these two concept documents lay the foundation that will support senior leaders as they assess needs and approve the development of solutions that will deliver future Joint C4 capabilities.

U.S. Strategic Command's (USSTRATCOM) Joint Task Force-Global Network Operations (JTF-GNO)[3] is responsible for the policy, guidance, and oversight that will transform today's Department of Defense's (DoD) information assets. We will move from a loose federation of inter-networked elements toward what will become the future capability – a robust Global Information Grid (GIG) Enterprise that will provide information where it is needed, when it is needed, and to those who need it most. Key to this transformation is the continued development of GIG Network Operations (NETOPS) policy and procedures. With the release of GIG NETOPS Version 2.0, JTF-GNO[4], working with the Joint Staff and all the *Combatant Commands* (COCOMs), lays the foundation for improving command and control (C2) relationships for network defense and operations throughout the GIG. JTF-GNO established a disciplined approach to network management that will enable the DoD to *operationalize*[5] the GIG.

The evolving net-centric environment has the potential to make joint networks our *Achilles heel*. Robust information assurance (IA) solutions are critical to providing the end-to-end capability that will deliver secure voice, data, video, and imagery. Trusted information must be accessible at all levels, including out to the *tactical edge* – at the right time, in the right format, and under every circumstance. Throughout 2005, Joint Staff Command and Control (J6) collaborated with the Assistant Secretary of Defense Networks and Information Integration/DoD Chief Information Officer (ASD [NII]/DoD CIO), Defense Information Systems Agency (DISA), JTF-GNO, COCOM, Services and other agencies[6] to improve our IA posture. As a result, department leadership awareness of existing cyber threats was significantly increased, and enterprise-wide security solutions for patching and conducting assessments were implemented (via the DoD IA/Computer Network Defense [CND] Enterprise Solutions Steering Group). The team also developed and implemented an IA annex to the Joint C4 campaign plan that provided the Joint community with a one-stop means for understanding and complying with IA policy and guidance.

The transformational vision of NCO requires a move from *stove-piped* and *interoperable* systems to interdependent systems. To achieve this end, the team focused on numerous information integration efforts. A key example is the partnership with the Office of the Secretary of Defense's Director of Operational Test and Evaluation, DISA's Joint Interoperability Test Command, and U.S. Joint Forces Command (JFCOM) to establish a joint network-centric test environment. By securing funding to conduct testing in a NCE, the process of linking interoperability testing with JFCOM's Joint National Training Capability training efforts was initiated. Another success came in the area of Joint C4 Interoperability Certification Process[7], where the Joint staff assessment was streamlined. By removing unnecessary interoperability certification reviews, COCOM and service staffing time was reduced, yet the net-worthiness of required joint C4 capabilities was still validated. Finally, review of interoperability issues affecting our warfighters in their current operating environments was increased. These reviews resulted in incorporation of Joint Operations lessons learned into interoperability test plans for 10 planned COCOM joint exercises. The work in this area will ensure lessons learned become lessons applied, and not lessons forgotten.

Any discussion of force transformation requires consideration of one of NCO's critical enablers: use of and access to the electromagnetic spectrum. Because spectrum remains a *high demand* but

increasingly scarce resource, the team has worked diligently during the past year with ASD (NII)/DoD CIO, to solve pivotal joint spectrum issues. The first concern related to providing the joint community, Military Services, and defense agencies with coordinated spectrum guidance. The result of this effort was the publication of the Spectrum Annex to Joint C4 campaign plan, an endeavor that provided our warfighting force with a strategy that defines, operationalizes, and will ultimately improve the management and use of the electromagnetic spectrum.

Spectrum-related issues of real-world operations were also examined. Many similar challenges were noted and solutions identified. As a result of this analysis, collaboration among departmental partners resulted in the creation of a dedicated spectrum Web site[8]. By making spectrum-related lessons learned more visible, our joint forces no longer had to waste valuable resources solving identified problems that already had proven remedies. We also went beyond analyzing spectrum issues. Again, working with our ASD (NII)/DoD CIO, COCOM, and service representatives, the team successfully obtained Joint JROC approval and funding for the development of two key spectrum management capabilities. The U.S. European Command sponsored Advanced Concept Technology Demonstration Coalition Joint Spectrum Management Planning Tool. When combined with the Global Electromagnetic Spectrum Information System program of record, spectrum managers at all levels will have the ability to plan and synchronize spectrum use to support operational demands on a near real-time basis, ensuring critical support to all spectrum-dependent missions.

Connectivity remained a 2005 priority and new transport and space capabilities were advocated. One of the lynchpins to successful NCO remains providing our joint forces with interoperability solutions that improve information flow throughout the battlespace. Creating this type of connectivity requires wireless solutions down to the *first tactical mile* with capabilities like the Joint Tactical Radio System (JTRS). Working with the COCOMS and Services, the JTRS program was re-scoped to ensure critical software definable radios will be delivered when needed to support joint warfighters. J6 also worked with ASD (NII)/DoD CIO and DISA to redefine the internet protocol (IP) environment regarding teleports. This effort will improve standardized tactical entry points and facilitate intra-theater and reach-back C4 capabilities for deployed forces throughout the world. Enhancing C2 systems continued to be a priority. J6 worked closely with the operational community to ensure the development of the Joint Command and Control System remains on track and enhancements continue to meet warfighter needs. Finally, worldwide, mobile access to satellite communications is crucial to current operations, as well as future NCO. A great deal of effort went into working with service and COCOM partners to advocate for and defend the funding of critical space capabilities that will be provided by initiatives such as the Advanced EHF system, Mobile User Objective System, and Transformational Satellite Communications System.

In late 2004, J6 met with service and COCOM representatives to discuss how to prepare Joint C4 planners to support real-world operations when deployed. While service C4 training was good, joint C4 training was virtually non-existent. Working with JFCOM and the Services and other COCOMS, the JROC approved development and implementation of a Joint C4 planners course. The course, which will be launched in 2007, will enable future Joint C4 planners to deliver the Joint C4 networks and capabilities that enable NCO.

Agenda for 2006

The key to success in 2006 will be constancy of purpose. Transforming Joint C4 capabilities to support future NCO will continue to be our focus.

The continued efforts of the Net-Centric Functional Capability Board and adherence to the JCIDS processes will ensure the foundational concept documents that were developed and approved in 2005 can be successfully leveraged. The first objective will be to complete the NCOE CBA – an effort that will result in a NCOE Joint Capabilities Document providing the contextual framework for service planners and developers to build the net-centric capabilities our joint forces will need in the year 2015 and beyond. Working closely with ASD (NII)/DoD CIO to complete the NCOE synchronization road map will also be a priority. This important analysis will enable the department to manage the delivery of baseline net-centric capabilities of the GIG and ensure their availability when and where the joint force needs them. Finally, working with USSTRATCOM and the JTF-GNO on improving the NETOPS Concept of Operations, as well as the joint NETOPS architecture, will continue.

As in 2005, 2006 activities will continue to support current and ongoing operations. J6, along with JTF-GNO, COCOMs, Services and agency partners will work to strengthen network command and control and NETOPS. At the same time, policies will be refined and exercises conducted to reflect evolving tactics, techniques, and procedures. Additionally, the entire Joint C4 community will work to improve the overall IA and CND posture in support of ongoing operations and initiatives. Finally, to strengthen current operations, end-to-end joint C4 configuration management will be improved. The focus will be on addressing roles, responsibilities, authorities, and governance structures affecting management control across the GIG.

To strengthen joint network security, the IA staff will continue to improve existing processes as well as work with key staff on critical initiatives in support of joint force IA requirements. For example, the C4 critical infrastructure protection assessments will be combined with IA assessments, creating a more holistic approach to managing initiatives used to protect networks.

In coordination with key department stakeholders, overarching policy in two key areas will be published. The first will streamline the acquisition processes and documentation related to developing security solutions for C4 systems. The second will implement DoD software assurance guidance. Strengthening information protection throughout the joint force will also be addressed. More specifically, the Joint C4 community has decided the time has come to accelerate Public Key Infrastructure (PKI) implementation to include developing and delivering signed and encrypted e-mail, smart card logon, and PKI authentication to Web servers. Senior Joint C4 leadership is committed to addressing concerns of our joint forces operating throughout the world. It is imperative that the problems experienced due to the lack of clear Joint Communications Security (COMSEC) policy and procedures be solved. The management and distribution of joint COMSEC materials used to support our warfighters will be improved.

Finally, two information sharing (IS) initiatives are underway. The first will develop a Joint IS strategy. The strategy must lay the foundation for transformational IS efforts and enable warfighters to make superior decisions in a timely manner. The second area will focus on IS programmatics with the objective of consolidating and standardizing the supportability and interoperability of current multinational systems including the Combined Enterprise Regional Information

Exchange System. The effort will also begin to formalize requirements for future multinational information sharing capabilities via the JCIDS process.

Key to the success of NCO is implementation of a comprehensive data strategy. Information integration was a priority last year and will remain one in 2006. For example, accelerating data strategy initiatives will be pursued in the following ways:

- By improving information sharing among the Services and Joint community on data strategy implementation.
- By promoting an understanding of data strategy guidance.
- By synchronizing Service approaches to facilitate a Joint process for community of interest (COI) governance.
- By establishing a formalized mechanism to coordinate warfighter domain data strategy efforts.
- By identifying gaps or issues in COI support of the warfighting mission area (WMA).

Other information integration areas will include Joint Interoperability metrics, testing, and validation. These efforts are essential for senior leaders responsible for making informed decisions regarding the lifecycle management of Joint C4 capabilities.

Electromagnetic spectrum will continue to be a Joint C4 priority in 2006. Without question, increasing awareness of issues related to spectrum and ensuring spectrum supportability requirements must be addressed early in the JCIDS and acquisition processes. Additionally, continuing to assist key departmental partners is part of the 2006 plan. Emphasis will be placed on establishing spectrum management training programs that prepare service spectrum managers to operate in the joint operational environment. Attention must also be given to creation of policies and methods to foster development and management of a qualified spectrum manager cadre. Finally, the Joint Staff will continue to work with COCOMS, Services and agencies to further the work being done by the Improvised Explosive Device (IED) Task Force including methods to mitigate the effects of IEDs on joint force operations.

Space and transport initiatives will continue to be a priority throughout the Joint Staff. Addressing space support will include reviewing the management process for commercial and military satellite communications. While conducting this review, refinements to software tools and processes allowing for greater accuracy, currency, and relevance of the information contained in the satellite communications database will be evaluated. Improving satellite support to the joint warfighter remains a top priority. Analysis of methods that could augment existing space capabilities will also continue. This will include consideration of new means to provide persistent, responsive, and dedicated *space-like* capabilities at tactical and operational levels to meet our growing joint force satellite communications requirements.

Other initiatives in 2006 will analyze methods to improve discipline in operations throughout the joint network. Since a risk assumed by one is a risk to all, working with JTF-GNO, COCOMS, and Services to ensure the commanders' capabilities to enforce network policy and procedures is essential.

Another area to be addressed is the department's ongoing effort to transition from IP Version 4 to IP Version 6 (IPv6). IPv6 will provide a virtually unlimited ability for the department to service addresses associated with the growing number of IP-enabled capabilities being developed to support NCO. Specifically, the communications-on-the-move capabilities that will be fielded will rely on the quality of service expected from IPv6. With a department goal to become IPv6 compliant by 2008, the staff will work with DISA, ASD NII/DoD CIO, COCOMS and Services to ensure the transition strategy is sound. Since funding constraints will require a phase-in of IPv6 capable assets over time, activities involving tests to ensure new and old systems are secure and compatible will be part of the transition strategy. Vigilance will be required to work with the key stakeholders to ensure our transition to IPv6-enabled capabilities does not disrupt ongoing operations.

Conclusion

The past few years have emphasized an improvement of network capabilities, especially with regard to secure information. Framing issues around operational terms has helped *de-mystify* the effect of C4 vulnerabilities on the warfighter, both now and in the future. We are committed to continuing a dialogue with the operational community to ensure an understanding of how pressing Joint C4 issues apply to and affect them. More importantly, we look forward to continuing to work with our Joint C4 Community partners to deliver the Joint C4 capabilities that will continually move the force closer to the NCO's vision for the future.◆

Notes

1. For more on JCIDS process, go to <www.dtic.mil/cjcs_directives> and see Chairman Joint Chiefs of Staff Instruction 3170.01E.
2. See <www.dtic.mil/futurejointwarfare> and click on JICs.
3. See <www.stratcom.mil> for more on JTF-GNO.
4. See <www.stratcom.smil.mil> for more on GIG NETOPS.
5. *Operationalize the GIG* means treating it with the same kind of rigor and discipline that is applied to other weapons systems and those who control or operate them.
6. See <www.defenselink.mil> to learn more about ASD (NII), DoD Agencies and Combatant Commands.
7. See <www.dtic.mil/cjcs_directives> CJCSI 6212.01C.
8. See <www.js.smil.mil>, J6, MCEB Secretariat, Spectrum Branch.

About the Author

Lt. Gen. Robert M. Shea serves as the Director, Command, Control, Communications and Computer Systems (C4 systems), The Joint Staff. He is the principle advisor to the Chairman, Joint Chiefs of Staff on all C4 systems matters within the Department of Defense. Shea's military service spans 33 years. Prior to his current assignment, he was the Deputy Commander, U.S. Forces, Japan. Shea's command positions include: Commander of the Marine Component to the Joint Task Force Computer Network Defense, Director of the Marine Corps Command and Control Systems School, Commanding Officer, 9th Communications Battalion, and I Marine Expeditionary Force during Desert Shield and Desert Storm. Other assignments include Commanding Officer of two communications companies and the Battalion Communications Officer for 1st Amphibian Tractor Battalion, 3rd Marine Division.

JS J6 DAG
ATTN: Col. Anderson or
Lt. Col. Patricola
The Joint Staff, J6-DAG
Washington, D.C. 20318
Phone: (703) 571-9750
E-mail: john.patricola@js.pentagon.mil or roarke.anderson@js.pentagon.mil

Overview of the Department of Defense Net-Centric Data Strategy

Anthony J. Simon
DoD CIO/Information Management Directorate

Net-centricity is the realization of a networked environment that includes infrastructure, systems, processes, and people. Net-centricity enables net-centric operations, a completely different approach to warfighting, intelligence, and business functions.

The Department of Defense's (DoD's) Global Information Grid (GIG) provides the foundation for net-centricity. The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, defense policy makers, and support personnel[1]. The information capabilities that comprise the GIG include transport, Web-based services, information assurance technologies, applications, data, architectures and standards, and the tools, techniques, and strategies for managing and operating the GIG (e.g., Network Operations [NetOps]). By securely interconnecting people and systems independent of time or location, we can achieve substantially improved military situational awareness, better access to information, and dramatically shortened decision cycles. Our warfighters are empowered to more effectively exploit information; more efficiently use resources; and create extended, collaborative communities to focus on the mission.

The approach to implementing the GIG uses communications, computation, information assurance, and Web technologies, but we also recognize that the cultural barriers against trust and data sharing must be addressed. Hence, the DoD is using a comprehensive, integrated approach to deliver the foundation for net-centricity. This approach combines the DoD Net-Centric Data Strategy[2], an information assurance (IA) strategy, and the implementation of communications, computing, and service layers that comprise the Enterprise Information Environment (EIE) of the GIG.

The core of the net-centric environment is the data that enables effective decisions. In this context, data implies all data assets such as system files, databases, documents, official electronic records, images, audio files, Web sites, and data access services. One of the goals is to populate the network with all data (intelligence, non-intelligence, raw, and processed) and change the paradigm from *process, exploit, and disseminate* to *post before processing*. All data is advertised and available for users and applications when and where they need it. In this environment, users and applications search for and pull data as needed. Alternatively, users receive alerts when data to which they have subscribed is updated or changed (i.e., publish-subscribe). Authorized users and applications have immediate access to data posted to the network without process, exploitation, and dissemination delays. Users and applications tag data assets with metadata, or data about data, to enable discovery of data. Users and applications post all data assets to *shared* space for use by others in the EIE. The environment shifts from private data to community of interest or EIE data as a result of increased data *sharing* in the net-centric environment.

Prior DoD approaches to data attempted to standardize and control data elements, definitions, and structures across the DoD, requiring consensus among and across all organizations. The approach intended to promote interoperability through standardization of data elements, minimize duplication of data elements across the DoD, and reduce the need for data element translation. The prior approach proved to be too cumbersome to implement across an enterprise as large and complex as the DoD.

The DoD's Net-Centric Data Strategy defines a new approach to data within the DoD. The strategy expands the focus to visibility (e.g., tagging) and accessibility (e.g., exposure services) of data rather than standardization. It recognizes the need for data to be usable for unanticipated users and applications, as well as known users. The strategy identifies approaches that will improve flexibility in data sharing, supporting interoperability between systems without requiring highly engineered, pre-defined, tightly coupled pair-wise interfaces between them. This flexibility will be essential in the *many-to-many* exchanges of a net-centric environment. While tightly coupled interfaces between systems will continue to exist (e.g., sensor-to-shooter systems that require real-time, direct communications to close the kill chain such as a weapons targeting system), the objective in a net-centric environment is to increase the potential for many other systems to leverage the same data without having to anticipate and engineer this use during the development cycle of the producer system.

For example, sensor-to-shooter systems can offer *exposure* services that work *behind the scenes* collecting real-time data, storing it, and providing access to other users (e.g., through Web services). Exposure services can be designed to have little or no effect on performance critical processes and still provide system data access to unanticipated users. In the dynamic environment that the DoD faces, one in which systems are continually being developed, deployed, migrated, and replaced, it is imperative that unanticipated interfaces can be accommodated quickly. It is also necessary that systems be designed to separate data from applications, and where practical, allow *loose coupling* between services that expose and exploit data.

This data vision, as codified in DoD Directive 8320.2[3], is predicated on several key elements that are critical to realizing a net-centric environment:

1. **Communities of Interest (COIs).** COIs are collaborative groups of users who exchange data in support of their shared mission and who must have a shared vocabulary to understand their data. COIs support users across the DoD by promoting data tagging, creating catalogs of metadata for their data, registering their metadata for others to use, and creating access services. Data of interest to a COI can be advertised only for use by the COI or across the EIE. COI catalogs, which describe the data assets that are available, are made visible and accessible for users and applications to search and pull data as needed. A guide for COIs to address the implementation of DoD 8320.2 is pending signature and will be available through the Defense Technical Information Center Web site and through the DoD Chief

Information Officer (CIO) public Web site. The DoD CIO public Web site[4] offers a variety of links to information to help DoD personnel become familiar with related topics such as COIs and implementation specifics.

2. **Metadata.** Data about data is important to achieve the data strategy goals of making data understandable and enabling interoperability. Discovery metadata that is compliant with the DoD Discovery Metadata Specification[5] provides a way for data to be found by DoD search capabilities. When COIs register their semantic and structural metadata in the DoD Metadata Registry, it can be used by others to support interoperability and provide a richer semantic understanding of the associated data. The DoD Metadata Registry site[5] is used by COIs to register their metadata agreements that allow others to understand the semantics and structures of their COI data. The DoD Metadata Registry site also contains guidance on implementing the visibility goal of 8320.2 including reference implementations for tagging.
3. **Core Enterprise Services.** Core Enterprise Services are a common set of services for the GIG that enable data sharing, searching, and retrieving. The planned set of core enterprise services includes discovery, collaboration, mediation, messaging, information assurance/security, storage, applications, user assistant, and enterprise services management. Each of these services provides core capabilities that enable warfighters and business users within the DoD to get access to the right information at the right time. In essence, the collection of these services is similar to those underlying the ubiquitous operation of the Internet. For example, at the most basic level, the discovery service provides the equivalent of Google to the Internet; messaging provides the equivalent of AOL's Instant Messaging; and information assurance/security provides the equivalent of Microsoft's Passport, a single sign-on to multiple Internet capabilities. In the DoD's case, these EIE services are based on commercial products and services, but configured to meet the response times required for our warfighter's mission critical needs and hardened through rigorous information assurance/security. By building the GIG on these common services, every warfighter and business user who knows how to navigate the Internet and use a Web browser will be able to exploit the GIG. More information about the net-centric enterprise services program being managed by Defense Information Systems Agency is provided at <http://www.nces.dod.mil/>.

DoD Directive 8320.2 requires that components begin implementing the policies in the data strategy, and it requires the DoD's governance processes (acquisition, capabilities identification, and planning and budgeting) be modified to promote data sharing. The FY2006-2011 Strategic Planning Guidance (classified) has required the components to begin planning for and resourcing activities to make data visible, accessible, and usable. The DoD CIO is providing implementation guidance for and working with components, COIs, and program managers to ensure that data sharing practices are understood and implemented. By working with COIs (e.g., COI forums and pilot programs), the DoD can share lessons learned and improve overall guidance for increasing net-centric data sharing.

As a result of the 2006 Quadrennial Defense Review, a Program Decision Memorandum was issued that directed the DoD CIO to provide a defense-wide report to the Deputy Secretary of Defense on progress and impediments to implementing the data strategy. The DoD CIO will be working with DoD components and the information technology portfolio managers defined in DoD Directive 8115.1[6] to highlight successes, capture best practices, and identify obstacles that have to be removed.

The National Defense Strategy, March 2005, requires that the DoD *will conduct network-centric operations with compatible information and communications systems, usable data, and flexible operational constructs.* The DoD Net-Centric Data Strategy is a critical element to net-centric operations. The data strategy is the cornerstone to ensuring that information can be found, accessed, and understood by those who need it. The DoD CIO will continue to work with the DoD components to implement this priority.

Notes

1. See Department of Defense Directive 8100.1. "Global Information Grid (GIG) Overarching Policy." Sept. 2002. <www.dtic.mil/whs/directives/corres/html/81001.htm>.
2. Department of Defense Net-Centric Data Strategy <www.dod.mil/nii/org/cio/doc/Net-Centric-Data Strategy-2003-05-092.pdf>.
3. See Department of Defense Directive 8320.2. Data Sharing in a Net-Centric Department of Defense. Dec. 2004 <www.dtic.mil/whs/directives/corres/html/83202.htm>.
4. Department of Defense Chief Information Officer <www.dod.mil/nii/coi/>.
5. Department of Defense Metadata Registry and Clearinghouse <https://metadata.dod.mil/mdrPortal/appmanager/mdr/mdr>.
6. See Department of Defense Directive 8115.1. Information Technology Portfolio Management. Oct. 2005. <www.dtic.mil/whs/directives/corres/html/811501.htm>.

About the Author

Anthony J. Simon led the development of the Department of Defense (DoD) Net-Centric Data Strategy, which has become a widely known and referenced document and is perhaps the best description of the envisioned future environment. He assists the DoD chief information officer in managing, directing, executing, overseeing, and implementing many facets of information management across the DoD. Simon is responsible for providing policy and guidance for the DoD's net-centric data sharing direction. He has nearly 20 years of information management experience and for the last 10 years, has served as a senior information technology specialist for the Office of the Secretary of Defense (Networks and Information Integration). Simon has also worked for the Defense Information Systems Agency and the Defense Intelligence Agency. He holds a Bachelor of Science degree from Virginia Tech in Management Science and a Master of Business Administration from Marymount University.

DoD CIO/ Information Management Directorate
1851 S Bell ST
STE 600
Arlington, VA 22202
Phone: (703) 602-1090
Fax: (703) 602-0830
E-mail: anthony.simon@osd.mil

Transformational Communications Systems for DoD Net-Centric Operations

Dr. Troy Meink
Office of the Assistant Secretary of Defense Networks and Information Integration

The Department of Defense (DoD) is moving ahead to establish the next generation of warfighting communications capabilities needed for global net-centric operations. The key programs that make up this new capability are the Transformational Satellite Communications System (TSAT), the Joint Tactical Radio System (JTRS), and the Defense Information Systems Network – Next Generation (DISN-NG). These programs will greatly enhance the ability of the DoD to share information – in real-time if required – improve command and control, and ultimately transform DoD operations. This article provides an update on the DoD's communications programs vision and status of the TSAT, JTRS, and DISN-NG programs.

The foundation for U.S. and coalition net-centric operations is the communications network. This vital *transport* system allows critical warfighter information to be shared real-time and will enable global net-centric operations. The heart of the Department of Defense's (DoDs) long term integrated investment strategy is a network of systems providing greatly enhanced capabilities for all aspects of U.S. national security activities. This includes persistent surveillance, distribution of detailed actionable intelligence, and support to precision strike. It also includes secure, protected, networking-on-the-move (NOTM) communications capability to support enhanced command and control of forces. This capability supports not only tactical forces, but also all other national security operations, including logistics, business operations, and intelligence functions. Several key programs will be integrated to provide an end-to-end communications capability to support net-centric operations (Figure 1). The key programs within these areas are the Transformational Satellite Communications System (TSAT), the Joint Tactical Radio System (JTRS) and the Defense Information Systems Network-Next Generation (DISN-NG) (Figure 2).

Transformation Satellite Communication System (TSAT)

TSAT is the cornerstone of the DoD's future communications network and provides real-time global reach. It is the spaceborne element of the Global Information Grid (GIG), and it enables secure, protected, networked, bandwidth-on-demand communications connectivity to fixed/mobile strategic and tactical users. The Army's *Future Force*, Navy's *SeaPower 21*, and Air Force's *Air Expeditionary Force* rely on the transforming capabilities of flagship systems including the Army's Future Combat System and Warfighter Information Network-Tactical, the Air Force's Space Based Radar (SBR) system, and the various Unmanned Aerial Vehicle platforms. The full capability of these systems depends on the space-based network connectivity TSAT will provide.

TSAT is the next generation of satellite communications (SATCOM) system and represents an advancement from the

Figure 1: *Communications Components*

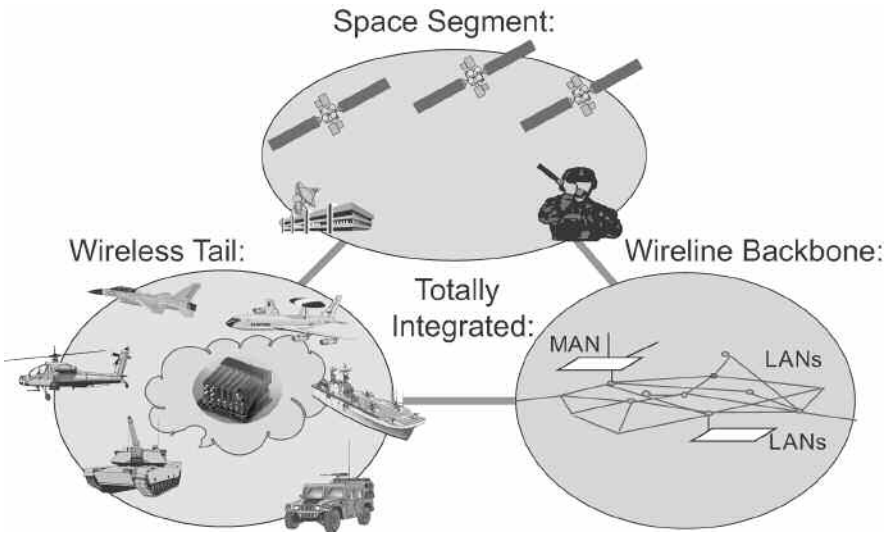
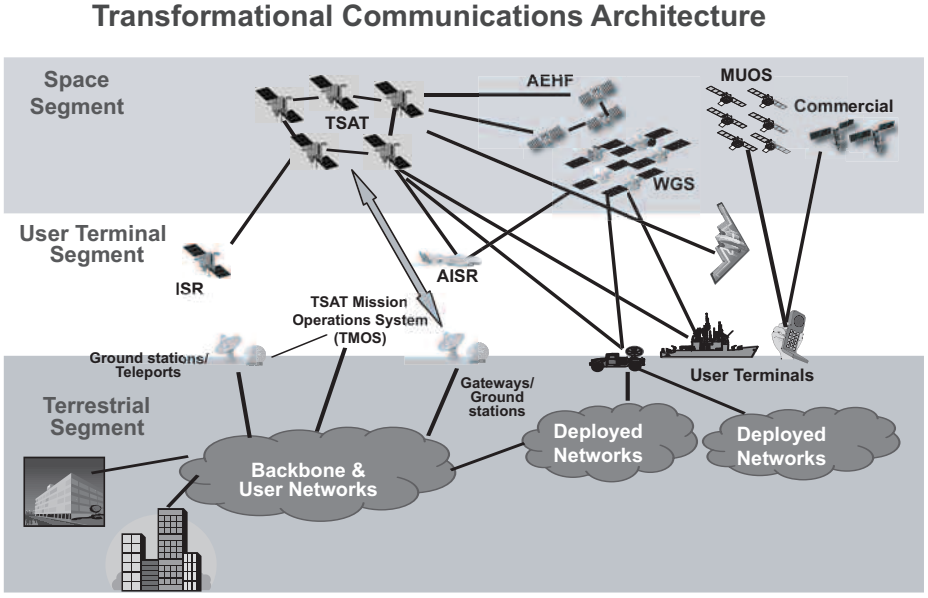


Figure 2: *Transformational Communications Architecture*



current circuit based systems such as Milstar, Advanced Extremely High Frequency, and Wideband Gapfiller System, to a fully networked system providing dramatically improved connectivity across the GIG. In addition, TSAT provides significant increases in data rates to small and large terminals enabling high data rate *protected* NOTM and support to airborne and spaceborne Intelligence, Surveillance, and Reconnaissance communications capabilities (e.g. SBR and Global Hawk). Figure 3 shows the evolution of capabilities from one generation of space systems to the next. For example, NOTM is one of the key new requirements that TSAT meets. This basic requirement is to be able to dynamically reconnect to a vehicle moving at 40 miles per hour with a 1.5 megabit per second (T1) communications link. This vehicle would have a one foot antenna. Only TSAT can meet this critical warfighter requirement.

The TSAT program made significant progress in fiscal year (FY) 2005. Given the Congressional direction resulting from the FY 2005 appropriated budget, the program renewed its focus on maturing the key subsystem technologies and plans to continue this focus through maturation to Technology Readiness Level-six (TRL-6) and beyond. The program office is verifying TRL status via testing of contractor developed hardware in an independent government testbed. In addition to technology maturity, these tests will demonstrate integrated performance of the TSAT system and support systems design activities. In FY 2005, three of the six key technologies were matured to TRL-6, and the remaining three technologies are on track to achieve TRL-6 prior to the award of the system development contract, an earlier point than achieved by previous space programs.

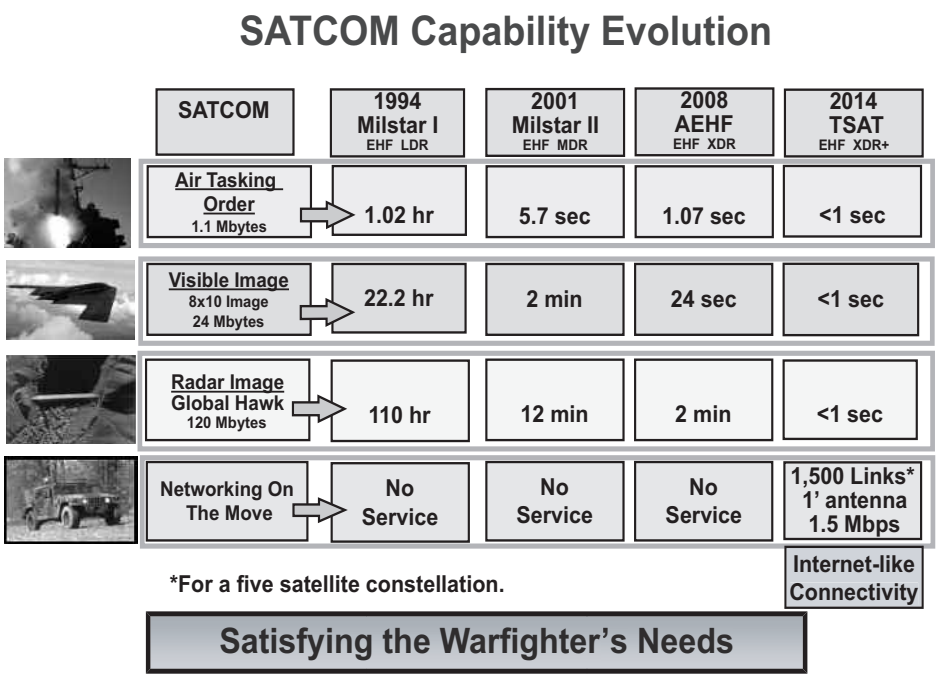
As part of the Quadrennial Defense Review, the DoD evaluated both the TSAT Program of Record (PoR) and a Block Build excursion from the PoR. The Block TSAT program delivers incremental capabilities in two blocks. In Block 1, the complexity and size of the payload are reduced significantly with respect to the PoR, and will simultaneously lower the development and integration risk. Taking a *smaller step* on the Block 1 satellites increases DoD confidence in launching these satellites on schedule and allows learning and performance to guide the Block 2 development.

The Undersecretary of the Air Force has made this block approach the model for other space programs to follow. We believe this new development paradigm will enable our ultimate goal – to efficiently acquire and deliver space systems that provide unique capabilities to our warfighter.

Joint Tactical Radio System

The JTRS program was initiated in early 1997 in response to the Services' pursuit of separate solutions to a programmable, modular, multiband, multimode radio that would eventually replace over 200 radio types in the DoD inventory. It is now considered the single DoD-wide approved program that will provide the next generation family of tactical radios to the warfighter with not only greatly expanded capabilities, but also increased interoperability through the incorporation of both existing and advanced waveforms. The family of radios will be scalable by virtue of form, fit and cost and will be expandable using the open software communications architecture (SCA) standard. The family will consist of three domains: airborne, ground, and maritime/fixed station. These domains are supported by five radio families (or *clusters*) to include handheld, man-packed, vehicular mounted, airborne and maritime/fixed station. JTRS lays the foundation for achieving net-centric connectivity across the below two gigahertz radio frequency spectrum. It provides the means for digital information exchanges between joint warfighting elements and enables connectivity across all domains of warfare – land, air, and maritime and also to civil and national authorities. JTRS also supports the need to share real-time information among joint warfighters and enables joint and combined interoperability and will support self-organizing, mobile, networked forces on-the-move. Using gateways if necessary, JTRS users can connect to other users beyond their line of sight via SATCOM. The SATCOM links then connect into the GIG, thus giving JTRS users on the front lines access to any information stored anywhere on the GIG.

Figure 3: *SATCOM Capability Evolution*



JTRS Waveforms. JTRS waveforms are managed by the JTRS Waveforms Program Office (JWPO). The purpose of the JWPO is to define, develop, validate, and evolve the JTRS SCA; acquire waveform software applications; acquire Crypto Equipment Applications; and perform architecture compliance testing of both JTR sets and waveform software.

JTRS Cluster 1 Program. The JTRS Cluster 1 Progam provides for development and production of the ground vehicular configurations of the JTRS radio family.

JTRS Cluster 2 Program. The JTRS Cluster 2 Program provides for development and production of a single channel JTRS handheld radio. This Cluster will modify the current MultiBand Intra-Team Radio (MBITR) for crypto and SCA compliance within the current spec-

trum parameters of the MBITR radios. This new version of the MBITR will be called the JTRS Enhanced MBITR or (JEM). Cluster 2 serves as an interim handheld until a JTRS Operational Requirements Document (ORD)-compliant two-channel, handheld, and man-pack radio that operates over the full JTRS spectrum is developed in Cluster 5.

JTRS Cluster Airborne, Maritime, Fixed/ Station (AMF). JTRS Cluster AMF provides for development and production of the airborne, maritime, and fixed family of JTRS radios. This program is still in a pre-system development and demonstration phase. Current plans call for award of the developmental contract in late 2006 (Cluster AMF combined the original Cluster 3 and Cluster 4).

JTRS Cluster 5 Program. The JTRS Cluster 5 Program provides for development and production of the handheld, man-pack and small form factor (embedded) configurations of the JTRS radio family.

Defense Information Systems Network - Next Generation (DISN-NG)

Prior to the implementation of the GIG, the DISN, the DoD's primary terrestrial transport system, was a collection of non-integrated dedicated transport subsystems. The subsystems were put in place to meet individual user requirements over the years and have grown to support a large customer base of military bases and installations worldwide. Although the name connotes a single network, the DISN actually consists of a number of separate networks and thousands of point-to-point leased circuits acquired to meet user's needs. The DISN supports the following six *DISN services*:

1. Unclassified internet protocol (IP) (NIPRNET).
2. Secret IP (SIPRNET).
3. Top-secret IP joint world wide intelligence communications system (JWICS).
4. Unclassified command and control (C2) voice service (Defense-Switched Network).
5. Video services, a secure command and control conferencing system for senior leaders (Defense Video Services – Global).
6. Secure C2 voice service and conferencing services (Defense Red-Switched Network).

The non-optimized attributes of the DISN resulted from decentralized budgeting issues, limitations on infrastructure investments, and technology limitations. The departments approach to terrestrial networks transformed dramatically in 2003 when the department was able to start a major investment to procure a fiber based Wide Area Network (WAN) transport system called the GIG Bandwidth Expansion program (GIG-BE).

The GIG-BE program provides a global fiber optic backbone as the primary terrestrial segment of an integrated communications transport architecture. GIG-BE creates a ubiquitous, robust, trusted network where terrestrial bandwidth availability will no longer be a constraint in providing, sharing, and using information. The GIG-BE connects 86 of the department's most important locations such as intelligence centers and force projection bases – those with the highest bandwidth requirements. It allows the department to reap the full benefits of other transformational investments in surveillance *reach-back* analysis, sensor-to-shooter integration, information and intelligence collaboration, and enterprise computing. GIG-BE's technical basis focuses on an IP network with significantly expanded bandwidth availability, where large quantities of information can be distributed, analyzed, and shared in new, more effective ways.

Now that the GIG-BE network is in operational status, the second step toward transformation is to extend the transport capabilities of the fiber WAN to the rest of the DoD and converge to a single network for all users. The migration of the DoD to an integrated net-centric terrestrial transport system will depend on the DISN-NG program. The goal is to have a truly integrated and converged IP network. The transition has started with the consolidation of IP based networks. Other service transitions efforts are focusing on voice-over IP and the transition of video services to IP, with a goal of full network convergence.

The final piece of the terrestrial infrastructure transformation is the link from terrestrial networks to satellites. The DoD teleport is linked to the DoD's fiber infrastructure and acts as the primary SATCOM gateway, providing access to numerous military and commercial satellites. The teleport provides tactical forces around the world with the ability to access and exploit the vast resources on the terrestrial net via satellites, providing a wide range of capabilities through global up and down links.

Conclusion

The foundation for U.S. and coalition net-centric capability is the transformational communications network. Without this vital *transport* system the warfighter/user information cannot support our operations. The heart of the DoD's long term integrated investment strategy is a network of systems providing greatly enhanced capabilities for all aspects of U.S. national security activities. This includes persistent surveillance, distribution of detailed actionable intelligence, and support to precision strike. It also includes secure, protected, NOTM communications capability to support enhanced command and control of forces. This capability supports not only tactical forces, but also all other national security operations, including logistics, business operations, and intelligence functions. Several key investment programs, including TSAT, JTRS, and DISN-NG will be integrated to provide an end-to-end transformational communications capability to enable net-centric operations and vastly improve future DoD operations.◆

About the Author

Dr. Troy Meink is currently the Director, Communications Office of the Assistant Secretary of Defense/ Networks and Information Integration and is responsible for oversight and policy of communications programs within the Department of Defense. Previously, Meink was the Transformation Satellite Communications System program director at the Military Satellite Communications Joint Program Office, Space and Missile Systems Center. He has a doctorate degree in aeronautical and astronautical engineering from Ohio State University.

Office of the Assistant Secretary of Defense (Networks and Information Integration)
Attn: Dr. Troy Meink
6000 Defense Pentagon
Washington, D.C. 20301-6000
Phone: (703) 607-0270
Fax: (703) 607-0276
E-mail: troy.meink@osd.mil

Development of a Ground Vehicle Maneuver Ontology to Support the Common Operational Picture

Dr. Paul W. Richmond
U.S. Army Engineer Research and Development Center

Curtis L. Blais
Naval Postgraduate School MOVES Institute

Dr. Niki C. Goerger
U.S. Army Engineer Research and Development Center

To meet information needs of operational commanders, user-centric applications will combine Global Information Grid (GIG) data and services to create a Common Operational Picture (COP). The COP, a single identical display of relevant information shared by more than one command, will facilitate collaborative planning and situational awareness. Land warfare decision-makers are particularly interested in ground vehicle mobility characteristics of the battlespace. This paper describes both the Mobility-COP, from which warfighters can assess the ability of forces to maneuver effectively under multiple environmental and tactical conditions, and a formal ontology design to achieve the Mobility-COP in the future GIG net-centric architecture.

The Global Information Grid (GIG) [1] is emerging as the next-generation architecture for making military command, control, communications, computers, intelligence, surveillance and reconnaissance information available as discoverable and callable services to a spectrum of users, software agents, and software systems. To meet information needs of operational commanders, user-centric applications will compose GIG data and services to create a Common Operational Picture (COP), defined in Joint Publication (JP) 3-0 [2] as, "a single identical display of relevant information shared by more than one command." The COP will facilitate collaborative planning and situational awareness. The COP will be a user-tailorable selection, organization, and display of information obtained from diversely distributed data sources and services. Users across the force will have confidence the information provided in their respective COPs is drawn from consistent, trusted sources across the network.

Land warfare decision-makers are particularly interested in representation of ground mobility characteristics of the battlespace. Using these characteristics, warfighters assess the ability of forces to maneuver effectively under multiple environmental and tactical conditions. This portion of the COP is termed the Mobility-COP. Although a subset of the overall COP, the Mobility-COP presents a challenging mix of information provided by decision aids, environmental databases, platform performance data, doctrinal behaviors, and process simulation. These sources of data and services use a variety of data models that need to be reconciled through metadata and data mediation and then merged to create the Mobility-COP. This article describes the Mobility-COP and discusses development of an ontology to represent the data and information requirements of the Mobility-COP within the GIG architecture.

Mobility-Common Operational Picture

Assured Mobility

Assured mobility is a Force Operating Capability identified in the U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-66 for future operational environment capabilities. It states the assured mobility framework:

> ... includes all those actions that guarantee the force commander the ability to deploy, move, and maneuver, by ground or vertical means, where and when desired, without interruption or delay, to achieve the intent. [3]

The assured mobility concept ties into the larger operational framework as an overarching enabler supported by the various battlespace functions, including Engineer Battlespace Functions of Combat Engineering (mobility, countermobility, and survivability), Geospatial Engineering, and General Engineering. Unification of data and information across the various battlefield operating systems (BOS) components requires unification of conceptual data models across software systems manipulating that information. Specifically, a common vocabulary and formalized semantics are needed to describe ground vehicle mobility data for software support to movement planning and mission monitoring. Design of the Mobility-COP ontology serves this purpose, identifying the common concepts relating ground vehicle mobility across the components in the operational framework for assured mobility.

The following are the four imperatives of assured mobility that are linked to the elements of combat power [4]:

1. Develop mobility input to the COP.
2. Establish and maintain operating areas.
3. Negate the influence of impediments on operating areas.
4. Maintain mobility and momentum.

The first assured mobility imperative, *develop mobility input to the COP*, serves as the impetus for defining the Mobility-COP. Armed with identified critical mobility elements for the COP, the commander will gain improved situational understanding through the use of geospatial tools that combine improved intelligence, surveillance, and reconnaissance capabilities with terrain data. Each of the four imperatives for assured mobility has implications for what mobility-related data and information are needed for the Mobility-COP. These concepts provide insights and serve as a guide for further analysis, organization, and scoping of the Mobility-COP.

More formally, the Mobility-COP is defined as a subset of the COP consisting of relevant movement and maneuver data and information shared by more than one command [5]. The Mobility-COP can be tailored for various users and includes data and information for mobility of individual combatants, ground vehicles, and autonomous/robotic vehicles. Interoperability across battle command systems and simulations for mission planning and embedded training cannot be achieved without effective sharing of data and computational services. Effective sharing implies

the ability to express concepts that can be understood by diverse data sources and services.

With the requirement to enable interactions across multiple existing, emerging, and rapidly adapting systems, it is no longer possible to hard-code all systems to a single common data model. In contrast, given a common core data model, it is feasible for multiple systems to use adaptors and mediation services to express system-dependent concepts in the common interchange language. For this reason, development of a formal ontology for the Mobility-COP will provide a defined vocabulary and common semantics to serve as the basis for required interoperability. Following GIG guidelines, subsequent submission of the ontology to the Department of Defense (DoD) Metadata Registry and Clearinghouse[1] will make the model available to other domains.

Elements of the Mobility-COP Ontology

The Mobility-COP design team initially conducted a review and analysis of doctrine, data structures, standards and systems regarding ground vehicle mobility and maneuver. This analysis resulted in an initial slate of data categories and features/attributes for the Mobility-COP. Other data sources and standards which provided sub-elements or attributes to the above categories were examined; these included the data dictionary of the Force XXI Battle Command Brigade and Below, the OneSAF Objective System (OOS) Environmental Data Model (EDM), as well as Commercial Joint Mapping Tool Kit Battlespace Terrain Reasoning and Analysis (BTRA) products. A systems engineering-based process was conducted to obtain input from subject matter experts and stakeholders as a critical part of determining the elements and a hierarchical structure. The assured mobility imperatives discussed previously and the Army Universal Task List were used as part of the process. Analysis of the inputs from the participants resulted in eight top-level categories of information defined in Table 1.

Emerging concepts and capabilities of the GIG, as well as current and emerging standards and tools, were investigated to define what is meant by a Mobility-COP relative to data, specifications, and Web services. To the extent possible, the Mobility-COP will reuse applicable standards, tools, and products rather than developing these over again. It is also not the intent of this work to define or redefine geospatial features and attributes that are found in existing standards, or to manipulate or normalize them. Recent publications by Dobey and Eirich [6] and Miller and Birkel [7] discuss issues associated with geospatial data and its representation and source, vis-à-vis the GIG. Our current intent is to represent terrain features within the Mobility-COP using the OOS EDM based on the Environmental Data Coding Specification (EDCS). The work of Dobey, Eirich, and Loaiza, [8] relating to environmental extension to the Command and Control Information Exchange Data Model (C2IEDM), using the EDCS, is also relevant to Mobility-COP development. Other related ontologies currently under development include a synthetic environment representation [9] and a DoD core taxonomy [10].

Mobility-COP Ontology Development

Noy and McGuinness [11] describe the development of ontologies in a step-by-step process. The first step is to determine the domain and scope of the ontology. We used their process, combined with subsequent analysis, to develop a hierarchal structure based on the BOS combined with competency questions (which a knowledge base should help answer). Based on the U.S. Army Operations Order format, an initial list of competency questions was generated:

- Where are the obstacles to maneuver?
- What are effects of terrain and weather on friendly (or enemy) ground vehicle maneuver?
- Where are the friendly (or enemy) avenues of approach?
- Where is the key terrain for friendly (or enemy) maneuver (e.g. mobility choke points, bridges)?
- What are the effects of observation and fields of fire on maneuver?

These questions assume that the area of operations and the mission are known in terms of the five W's [12]: who, what, when, where, and why. This leads to the next step in the development of an ontology: the reuse of existing ontologies. The C2IEDM is an internationally accepted data model[2], and recent studies have investigated the development and sufficiency of the C2IEDM ontology [13]. Although the concepts of maneuver analysis and mobility are not well represented, it offers much of the context required for the Mobility-COP ontology.

Tolk and Blais [14] describe a taxonomy as *a tree structure of classifications for a given set of objects*, and an ontology as *an*

Table 1: *Mobility-COP Top-Level Categories*

Categories	Definitions
Terrain	The natural and manmade features and their attributes that may influence mobility or manuever of ground vehicles.
Obstacles	Those terrain features or other objects or conditions that disrupt or impede movement of ground vehicles.
Weather	Current and forecasted weather conditions that affect mobility and maneuver (visibility, precipitation).
Maneuver Analysis	The results of an analysis to ground vehicle movement relative to mission, command and control, local culture, and other considerations. Also includes information classes required for the analysis.
Route Planning	A route plan (directions for moving from A to B), the results of intermediate steps to obtain the plan and a subset of the required data.
Threat Analysis	The location, capabilities, and other information (potential actions) relating to threats to maneuver that can include, in addition to enemy forces, local populations, and cultural effects.
Forces	Information relating to manuever and transportation units, and individual platform locations and capabilities as related to mobility and maneuver.
Utilities	Information (metadata) that may be applicable to all elements of the Mobility-Common Operational Picture.

attempt to formulate an exhaustive and rigorous conceptual schema within a given domain. A key distinction is that an ontology is not limited to a tree structure, but can represent a multiple inheritance hierarchy. For example, the subclass Minefield may simultaneously be considered a member of the Obstacle class while also being a member of a terrain or facility class. It would inherit some properties from each superclass.

Table 1 presents the top-level components defined thus far. The following provide descriptions of those components as they pertain to ground vehicle mobility and maneuver analysis.

Terrain

The terrain component of the Mobility-COP data model is defined as the natural and man-made features and their attributes which may influence mobility or maneuver of ground vehicles. Terrain includes natural and man-made features, where man-made features include minefields, bridges, roads, etc. Man-made objects are *things on, in, or over the terrain* (such as roads, tunnels, and bridges, respectively) and need to be distinguished from the underlying physical terrain (ground and water). Due to the extensive past and present work in the area of terrain data modeling, numerous representations are readily available that meet portions of Mobility-COP requirements. These models have many complementary representations that can be mined for use in the Mobility-COP; however, they also possess conflicting representations that need to be resolved for use in the Mobility-COP.

Obstacles

Obstacles consist of those terrain features or other objects or conditions which disrupt or impede movement of ground vehicles. As with terrain, obstacles may be natural (cliff, ravine, swamp) or man-made (minefield, log barricade, rubble). Some Terrain objects, whether man-made or natural, can also belong to the Obstacles class based on characteristics that cause these objects to disrupt or impede movement of ground vehicles. With an automated reasoner[3], members of various classes can be automatically classified as obstacles based on their properties; for example, a river with certain width and depth values can be classified as an obstacle. If those property values change, say during a drought, then the river may cease to be an obstacle. Obstacles are also fully specified in existing data models (e.g., Table 2) and can be reused for Mobility-COP purposes.

Weather

Weather consists of current and forecasted weather conditions, which effect mobility and maneuver (visibility, precipitation). This component has a similar structure to Terrain in that it is best characterized as a geographic region having certain physical and temporal characteristics. There are numerous data representations that meet Mobility-COP information requirements.

Maneuver Analysis

Maneuver Analysis includes the results of analyses related to ground vehicle movement with respect to mission, command and control, local culture and other considerations. Some researchers have observed that efforts to reach common terrain and environment models have been focused at the data level rather than at the information or knowledge level. The distinction is important. Systems have primarily dealt directly with the raw data characterizing a geographic region, performing various processing to derive some battlefield effect (such as line-of-sight). Rather than having such information available directly, numerous systems spend processing resources to derive the higher-order effects and often compute those results over and over again. Moreover, the raw data are extremely large, making it very inefficient to distribute over a network. What most systems really require is not the raw data itself, but the derived products (e.g., a geometric line-of-sight envelope). In recognition of this fact, the U.S. Army Engineer Research and Development Center's Topographic Engineering Center is defining a data model for a Geospatial Battle Management Language that:

> ... seeks to abstract and represent terrain and dynamic environment through a rich set of discrete objects (spatial and temporal) and relationships to tactical entities and tasks. [15]

The effect will be to reduce large terrain data sets to their tactical essence and express the reduction in an ontology for interoperability at the conceptual level. This work has clear relevance to the Mobility-COP ontology design effort.

Route Planning

Route Planning contains the route plan (directions for moving from A to B), the results of intermediate steps to obtain this plan, and a subset of the required data. Derivation of the routes is dependent on information from the other

Table 2: *Attributes of the OneSAF Objective System Environmental Data Model Minefield Area Feature[4] (a region throughout which explosive mines have been laid)*

Attribute Name	Description[5]
CASE_BURIAL_FRACTION	The fraction of the case that is buried beneath the terrain.
COMPLETION_PERCENTAGE	The extent of completion in terms of fractional ascension from start of construction to completion of construction.
DURATION_OVERVIEW	The quantity of time in gross sense that the minefield may be assumed to be active.
EXPLOSIVE_MINE_TYPE	The type of explosive mines (e.g. anti-tank, anti-personnel).
FORCE_IDENTIFIER	A textual identifier of a military or civilian force (which created the minefield).
GENERAL_DAMAGE_FRACTION	The extent of damage to the minefield in terms of fractional degradation from a fully functional state.
MINE_ALLEGIANCE	The military allegiance of the force responsible for the creation or maintenance of the minefield.
MINE_DENSITY	The areal density of explosive mines within the minefield. Units of one mine per square meter.
MINEFIELD_MARKING_TYPE	Specifies by who and how the minefield is marked.
NUMERIC_OBJECT_IDENTIFIER	The numeric identifier.
PREPARED_EXPLOSIVE_DESTRUCTION _COMPLETION_FRACTION	The extent to which the minefield has been prepared for destruction by explosives in terms of fractional completion.
SOURCE	The source from which the data were captured or upgraded.
UNIVERSALLY_UNIQUE_ID	Universally unique identifier, guaranteed to be unique to a specific machine (computer) at a specific time.

Mobility-COP categories; for example, slope information from terrain, minefield placement and status from obstacles, precipitation and temperature from weather, or mission and own-force mobility assets from forces. The BTRA software is a current decision aid performing this type of processing to generate route plans. Because the routes are products of such processing, BTRA can become a software service providing input to the Mobility-COP in the GIG environment.

Threat Analysis

Threat analysis from the Mobility-COP point of view describes ways in which the adversary can potentially disrupt mobility and maneuver during the course of a mission. In general, these can include areas to be avoided (when safe routes are desired) or approached (when the mission is to attack). For example, a fast, safe route through an urban area may need to include (in route planning) not only information regarding historical improvised explosive device locations, but also local market events (time and location). The challenge is to be able to express not only known threats (the physical location of an enemy force), but also the probability that the force will attempt to disrupt a mission.

Forces

The Forces component describes information relating to maneuver and transportation units, and individual platform locations and capabilities as related to mobility and maneuver. Since the representation of military forces is a key element of Command, Control, Communications, Computers, and Intelligence and modeling and simulation (M&S) systems, there are numerous representations available for reuse in the Mobility-COP data model. Clearly applicable are the XML schema representations used in the Defense M&S Office Unit Order of Battle Data Access Tool and the Military Scenario Definition Language (MSDL). MSDL is used for scenario initialization and scenario archival storage in OOS and has recently transitioned to product development status in the standardization process of the Simulation Interoperability Standards Organization. Taxonomies of military forces are also available in the DoD Metadata Registry and Clearinghouse.

Utilities

Utilities refer to information (metadata) that is applicable to all elements of the Mobility-COP. Since the Mobility-COP will be a specialized collection of information and services from the distributed data environment rather than a specific physical data structure on the network, the individual components making up the Mobility-COP will be discoverable in their own right through adherence to the DoD Discovery Metadata Specification[1]. Furthermore, specification of Mobility-COP will include not only metadata descriptions of data products, but will also specify Web-based processes using standards adopted for use in the GIG such as the Web Services Description Language. Currently missing from identified GIG standards is emphasis on stronger semantics for data and service description and service composition through the use of semantic Web constructs such as the Web Ontology Language and the Web Ontology Language for Services. Full specification of the Mobility-COP will include such representations to solidify the foundation for enhanced interoperability.

Summary

The Mobility-COP ontology is a specification of those elements within the domain of ground vehicle mobility and maneuver analysis essential for military decision making, battle command and simulation. It provides a representation of ground vehicle mobility data within the tenets of the COP and the GIG.

To help achieve assured mobility for the Future Force in a net-centric environment, the ability to publish, access, process, and disseminate mobility and maneuver-related data, and information among battle command, modeling, and simulation systems is imperative. To accomplish this facet of interoperability, a data model and formal ontology are being developed. Eight high-level categories and respective sub-elements have been identified based on doctrinal review, needs analysis utilizing input from military subject matter experts, and functional decomposition of tasks relevant to assured mobility based on the Army Universal Task List. A significant component of the remaining work involves determining which elements are unique to the Mobility-COP ontology and which are available from existing or emerging ontology development. The results will be continuously vetted with the community and cross-checked with other existing ontology, data model, and standards development efforts.◆

Acknowledgments

This project was funded by the U.S. Army Engineer Research and Development Center <www.erdc.usace.army.mil/>, and the Battle Command Simulation and Experimentation Directorate of the U.S. Army Deputy Chief of Staff G-3.7 <www.amso.army.mil/index.htm> through the Simulation to Command, Control, Communications and Computers Interoperability Overarching Integrated Process Team.

Disclaimer

The contents of this report are not to be used for promotional purposes. Citation of trade names does not constitute an official endorsement or approval of the use of such commercial products. All product names and trademarks cited are the property of their respective owners. The findings of this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

References

1. Department of Defense. Defense Acquisition Guidebook. Washington, D.C., 2004 <http://akss.dau.mil/dag/Guide book/Common_Interim Guidebook. asp>.
2. Joint Chiefs of Staff. Doctrine for Joint Operations JP 3-0. Washington, D.C. 2001. <www.dtic.mil/doctrine/jel/new _pubs/jp3_0.pdf>.
3. Department of the Army. Military Operations Force Operating Capabilities. TRADOC Pamphlet 525-66. Fort Monroe, VA: U.S. Army, Training, and Doctrine Command, 2003.
4. Department of the Army. Field Manual 3-34, Engineer Operations. Washington, D.C.: Jan. 2004.
5. Blais, C.L., N.C. Goerger, P.W. Richmond, B. Gates, and J. Willis. "Global Information Grid Services and Generation of Mobility Common Operational Picture." Proc. of the Simulation Interoperability Workshop, Orlando, FL: Mar. 2005.
6. Dobey, V., and P. Eirich. "The Challenge of Environmental Data Interoperability on the Global Information Grid." Proc. of the Simulation Interoperability Workshop, San Diego, CA: Mar. 2005.
7. Miller, D., and P.A. Birkel. "Reflections on 'The Challenge of Environmental Data Interoperability on the Global Information Grid' by Dobey and Eirich (05S-SIW-133)."

Proc. of the Simulation Interoperability Workshop, Orlando, FL: Sept. 2005.
8. Dobey, V.T., P.L. Eirich, and F.L. Loaiza. "Integration of Environmental Extensions into the C2IEDM (Methodology and Lessons Learned)." Proc. of the Simulation Interoperability Workshop, Orlando, FL: Sept. 2005.
9. Bhatt, M., W. Rahayu, and G. Stirling. "Onto: A Web Enabled Ontology for Synthetic Environment Representation Based on the SEDRIS." Proc. of the Simulation Interoperability Workshop, Orlando, FL: Sept. 2004.
10. Taxonomy Focus Group. Core Taxonomy Stubbing Exercise, An Examination of Connecting Community of Interest Taxonomies to a Core Taxonomy. Defense Information Systems Agency, Vers. 0.95: Mar. 2005.
11. Noy, N.F., and D. McGuinness. Ontology 101: A Guide to Creating Your First Ontology. Knowledge Systems Laboratory, Stanford University: 2001. <http://protege.stanford.edu/publications/ontology_development/ontology101-noy-mcguinness.html>
12. Carey, S.A., M.S. Kleiner, M.R. Hieb, and R. Brown. "Standardizing Battle Management Language – A Vital Move Towards the Army Transformation." Proc. of the Simulation Interoperability Workshop, Orlando, FL: Sept. 2001.
13. Turnitsa, C., and A. Tolk. "Ontology of the C2IEDM – Further Studies to Enable Semantic Interoperability." Proc. of the Simulation Interoperability Workshop, Orlando, FL: Sept. 2005.
14. Tolk, A., and C. Blais. "Taxonomies, Ontologies, and Battle Management Language – Recommendations for the Coalition BML Study Group." Proc. of the Simulation Interoperability Workshop, San Diego, CA: Mar. 2005.
15. Galvin, K., M.R. Hieb, A. Tolk, C. Turnitsa, and C. Blais. Coalition Battle Management Language Study Group Final Report. Simulation Interoperability Standards Organization, Orlando, FL: Sept. 2005.

Notes

1. The DoD Metadata registry and the Metadata Specification can be found at: <http://diides.ncr.disa.mil/mdregHomePage/mdregHome.portal>.
2. The C2IEDM documentation is available at <http://www.mip-site.org/>.
3. Reasoner: Something that can find new facts from existing data (also known as reasoning) <http://en.wikipedia.org/wiki/Reasoner>. See <http://www.w3.org/2004/OWL/> for a list of available reasoners.
4. See the Environmental Data Coding Specification at <http://sedris.org> for exact definitions.
5. Area feature type (in this case a minefield) is a property of an areal primitive feature, other properties of the primitive feature contain the location and extent information (see <www.sedris.org/drm.htm>).

About the Authors

Paul W. Richmond, Ph.D., P.E., is a mechanical engineer at the U.S. Army Corps of Engineers, Engineer Research and Development Center where he develops ground vehicle mobility models for use in simulations, simulators and performance analysis models, specifically related to terrain interaction and off-road performance.

U.S. Army ERDC
CEERD-GM-M
3909 Halls Ferry RD
Vicksburg, MS 39180-6199
E-mail: Paul.W.Richmond@erdc.usace.army.mil

Curtis L. Blais is a member of the research faculty in the Modeling, Virtual Environments, and Simulation (MOVES) Institute at the Naval Postgraduate School (NPS) in Monterey, Calif. Blais is currently working on a number of research efforts in the application of Web-based technologies to military modeling and simulation, command and control, and decision-making systems. Blais has a master and bachelor degree in mathematics from the University of Notre Dame, and is currently a doctoral candidate in MOVES at NPS.

Naval Postgraduate School
MOVES Institute
700 Dyer RD
RM 265
Monterey, CA 93943
E-mail: clblais@nps.navy.mil

Niki C. Goerger, Ph.D, is a research engineer with the U.S. Army Corps of Engineers, Engineer Research and Development Center. Her expertise is in the area of physics-based and effects-based representation and quantitative analysis in modeling and simulation (M&S) for military applications. Goerger is currently a research associate at the U.S. Military Academy and serves as the Academy's Defense Model and Simulation Office visiting professor with research tracks in lifecycle acquisition management; M&S and Command, Control, Communications, Computers, intelligence, surveillance, and reconnaissance interoperability; and physics-based representation in urban operations.

U.S. Army Engineer Research and Development Center
ATTN: GM-M
3989 Halls Ferry RD
Vicksburg, MS 39180
E-mail: niki.c.goerger@erdc.usace.army.mil

e-Dorado: The Lost Centric City of Information

My last BACKTALK article, *Transform This*, in the May 2006 issue of CROSSTALK, addressed the clarion call of transformation within the Department of Defense (DoD). This month, I tackle the *Holy Grail* of the transformation crusade: Net-Centricity. First, a parallel look at crusades and exploration.

In their quest for El Dorado, Spanish conquistadors documented large populations and great cities along the banks of the Amazon River. For 500 years, explorers and archeologists have been probing Brazil for traces of the lost cities of the Amazon. One of the more obsessed explorers was British archaeologist, Col. Percy Harrison Fawcett. Col. Fawcett was a surveyor in the British secret service and friend of Arthur Conan Doyle who later used his stories as inspiration for his work "Lost World."

Fawcett led seven expeditions up the Amazon River basin between 1906 and 1924 for the Royal Geographic Society. Fawcett studied ancient maps, legends, and records and was convinced there was a lost city somewhere in the Mato Grosso region of Brazil. In 1925, Fawcett took his son Jack and Jack's friend Raleigh Rimmell with him to look for a lost city he named Z. Jack depicted Z in his sketches as a large statuesque city of stone rising out of the jungle.

Fawcett sent a telegraph on May 29, 1925 to his wife explaining that he was going into unexplored territory. The three men were last seen crossing the upper Xingu, a southeastern tributary of the Amazon River. They were never heard from again. No sightings, no messages, no remains, and no city were found unless you talk to University of Florida anthropologist Michael Heckenberger.

Heckenberger's University of Florida team used maps, a Global Positioning System (GPS), and knowledge from members of the indigenous Kuikuro tribe to identify and map out 19 villages into two large clusters within a 386 square mile area where Fawcett disappeared.

Overgrown by jungle, the villages connect by roads some 50 yards wide in a grid-like pattern around a hub dotted with causeways, plazas, and other structures. The biggest villages included 200-acre residential areas, and the clusters supported populations of 2,500 to 5,000. The entire area in and between major settlements was carefully engineered and managed. Heckenberger believes the network of villages is one of the lost cities of the Amazon.

How did relentless explorers and enlightened scientists miss the cities beneath their feet? Ironically, their myopic vision of stone cities rising vertically up from the jungle floor obscured the possibility of an indigenous metropolis extending horizontally out into the jungle.

Fast forward to the 21st century and we find the DoD searching for a new city. The Office of the Secretary of Defense describes a net-centric city of information as:

> ... an information superiority-enabled concept of operations that generates increased combat power by networking censors, decision-makers and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability and a degree of self synchronization. [1]

This modern-day e-Dorado with a boatload of *ilities* sounds nice, but can it be done?

Net-centric technology is available, sound, and used commercially. Will it flourish in the defense community or succumb to parochial natives and bureaucratic overgrowth, disappearing into a jungle of politics? I am not sure, but here are some questions to explore. Net-centric success depends on a clearly defined vision or architecture. Col. Fawcett entered the jungle with scant notes and his son's drawings. Fawcett's myopic drive to find a stone city rising up from the jungle floor blinded his mind to the possibility of a network of villages that meet all the criteria of a thriving metropolis. Is there clarity in the DoD's net-centricity vision? Does the vision inspire, motivate, and enlighten or does it offer a list of platitudes? Does the vision allow for unconventional solutions? As with all technology adoption, the DoD will need to bridge the gap of doubt from concept to implementation. Is it a wobbly bridge of rope or a bridge over the river Kwai?

Net-centric success will depend on collaboration between the innovative roots of the armed Services and the canopy of defense leadership on a scale never achieved before. Comparing Fawcett to Heckenberger, I see two striking differences that stand out: The most obvious is Heckenberger's technological advantage in gear, maps, and GPS.

Less obvious is Heckenberger's resolute respect for the local natives by living with and helping them first. Fawcett, on the other hand, offered trinkets and gifts for native support. While initially effective, Fawcett's trinkets washed away while crossing a raging river. Heckenberger's partnership proved more stable and long lasting. Likewise, any technological advancement – while inspired and funded from the top – will come from the grassroots of each service. Can DoD leaders go beyond a funding relationship and establish stable, long-term partnerships with the native roots of innovation within the Army, Navy, and Air Force?

Finally, net-centric success depends on collaboration between the DoD and its suppliers. Defense contractors, which name I am sure derives from the word conquistador, naturally see net-centricity as a source of contractual gold. Marching through the acquisition jungle with brute force in quest of e-Dorado, contractors can lose sight of the desires of the natives, chiefs, and communities they serve. Rather than blaming conquistadors for being conquistadors, can the DoD harness the contractor's aggression, zeal, and force to meet net-centric goals?

Will net-centric warfare become reality? No doubt, the telegraph has been sent: We have crossed the upper Xingu into unexplored net-centric territory. The last question: Will we be lost in overgrown jungles of parochialism, bureaucracy, and politics or emerge with shared awareness, higher tempo of operations, greater lethality, and increased survivability? Lace up your boots and sharpen your machete. Lost cities are lost only because they have not been found.

— Gary A. Petersen
Shim Enterprise, Inc.
gary.petersen@shiminc.com

Reference

1. Office of the Secretary of Defense. "Transforming America's Military: Net-Centric Warfare." Washington, D.C.: 2005.

CrossTalk is co-sponsored by the following organizations:

Homeland Security

NAVAIR

CrossTalk/517 SMXS/MDEA
6022 Fir AVE
BLDG 1238
Hill AFB, UT 84056-5820

PRSRT STD
U.S. POSTAGE PAID
Albuquerque, NM
Permit 737